CAUSE NO. _____

THE STATE OF TEXAS, Plaintiff,	§ § §	IN THE DISTRICT COURT OF
v.	§ §	MIDLAND COUNTY, TEXAS
GOOGLE LLC, Defendant	§ §	____ JUDICIAL DISTRICT

PLAINTIFF'S ORIGINAL 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"), complains of Defendant GOOGLE LLC ("GOOGLE," the "Company," or the "Defendant"), and for causes of action would respectfully show as follows:

I. INTRODUCTION

For more than a decade, Texas has prohibited companies from capturing Texans' biometric data—including the unique characteristics of an individual's face and voice—without their informed, advance consent. In blatant defiance of that law, Google has, since at least 2015, collected biometric data from innumerable Texans and used their faces and their voices to serve Google's commercial ends. Indeed, all across the state, everyday Texans have become unwitting cash cows being milked by Google for profits.

Many Texans do not realize that their contributions to the tech giant's financial growth include offering up for inspection two of the most uniquely personal features any individual has to call their own. The proliferation of the commercialization of Texans' personal biometric identifiers is as invasive as it is dangerous. Unlike passwords, credit cards, Social Security numbers, and even names, biometric identifiers (like face geometry and voiceprints) form an inherent part of our unique, human identity and cannot be simply erased or replaced when stolen. Indeed, in 2011, Google's then-CEO Eric Schmidt warned that facial-recognition technology risked "crossing the

creepy line" and assured the world that Google "would not build a database capable of recognizing individual faces."[1] Today, Google has a new CEO and a new ethos, having tossed CEO Schmidt's promises into the rubbish heap alongside Google's abandoned "don't be evil" mantra. Google has now spent years unlawfully capturing the faces and voices of both non-consenting ***users*** and ***non-users*** throughout Texas—including our children and grandparents, who simply have no idea that their biometric information is being mined for profit by a global corporation.

Since at least 2015, Google has offered a feature it calls "Face Grouping" in its cloud-based Google Photos app. As the name implies, the feature employs facial-recognition technology. The technology works by first detecting all faces depicted in a photo or video loaded into Google Photos. When Google detects an individual's face, Google creates a record, or a face template, for that specific face. Google then evaluates whether the faces detected in each new photo or video uploaded is similar to face templates Google has previously recorded from other photos and videos. Finally, Google groups together any photos and videos depicting similar faces—known as "face groups"—based, in part, on the similarity of face geometry.

In 2015, Google researchers released a paper describing a deep-neural network called "FaceNet, that directly learns a mapping from face images to a compact Euclidean space where distances directly correspond to a measure of face similarity," allowing "tasks such as face recognition, verification and clustering."[2] "Euclidean space" is the fundamental two- or three-dimensional space in classical geometry. Google introduced FaceNet, in other words, as a tool to better capture an individual's unique face geometry. Upon information and belief, FaceNet is the engine behind Google Photos' ability to detect and map the geometry of millions of faces

[1] Matt Warman, *Google Warns Against Facial Recognition Database*, THE TELEGRAPH (May 18, 2011), available at http://www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition- technology.html.
[2] Schroff, Florian, et al., "FaceNet: A Unified Embedding for Face Recognition and Clustering," June 7, 2015, *available at* https://ieeexplore.ieee.org/document/7298682.

throughout Texas.

The Google Photos app is a runaway success for Google. The Google Play Store claims Google Photos has ***over five billion installs***.[3] The Apple App Store reports that over 339,000 users have submitted reviews of Google Photos.[4] Given that many installers do not submit a formal review, one assumes that the number of installs of Google Photos out of the Apple App Store is of the same magnitude or greater than installs out of the Google Play Store.

Against this pervasive backdrop of Google Photos, many Texans do not know or understand that Google powers Google Photos by recording and analyzing sensitive biometric information. But, even more striking is the fact that, through the Face Grouping process, Google captures and stores sensitive biometric data about Texan users and non-users alike—and Google stores that data for an unreasonable amount of time. When a Texas mother uploads photos of her daughter's third birthday party to Google Photos, for example, Google captures the face geometry of every child's face that can be detected in those photographs. Even more troubling, when the mother uploads video of the birthday party, Google runs facial recognition on every face detected in that video, including the faces of uninvolved bystanders in the park, restaurant, or schoolyard. And when a grandson drives to Midland to visit his grandmother on Easter and sends a series of photos taken on his Android phone to the family thread, those photos are sent to Google Photos by default, where Google captures grandma's face geometry. To Google, it does not matter that the three-year-olds, the bystanders, and grandma never consented to Google capturing and recording their biometric data.

For Google, it is immensely valuable for Texans to continue uploading photos and videos of themselves and their non-consenting friends and family members. Each time Google's

[3] *Google Photos*, GOOGLE PLAY STORE (last visited February 14, 2022).
[4] *Google Photos*, APP STORE PREVIEW (last visited February 14, 2022).

technology scans and analyzes a face—even the face of an unknown bystander—Google becomes better at scanning and analyzing faces. This machine-learning method drives Google's self-evolving technological growth, which in turn positions Google to maintain its dominance in the technology and consumer-products space. The ability to more accurately identify and analyze faces is an important piece of Google's commercial strategy, as demonstrated by the company's creative efforts in the past to build its collection of face scans.

Indeed, Google goes to extraordinary—and disturbing—efforts to enhance its "data." For example, several years ago Google hired contractors to engage individuals on the street in an attempt to gain permission to scan the strangers' faces. When Google wanted to build its database of people of color, Google's contractor reportedly targeted the homeless community. Google's Senior Vice President of Hardware, Rick Osterloh, has said Google "went out and did a lot of research in this area" because Google wanted "to get a large number of data points that allowed us to perfect" Google's facial-recognition model.[5] Notably, throughout that particular biometric-harvesting project, Google reportedly kept individuals' names and contact information segregated from their biometric identifiers, demonstrating that a biometric identifier alone, *even when decoupled from an individual's name*, is critical and valuable to Google's commercial endeavors.

Google runs a similar, yet expanded, playbook on other Google products—both hardware and software. A recent example is Google's Nest Hub Max. This commercial product is a multifunctional household device with audio and visual components that allows users to see and use various applications, search the internet, play music, view the weather, make calls, and so on. One of the Nest Hub Max's features is called "Face Match." Face Match uses facial-recognition technology to allow the Nest Hub Max to see who is using the device and to populate user-specific

[5] Leo Kelion, *Google Chief: I'd Disclose Smart Speakers before Guests Enter My Home*, BBC NEWS (Oct. 15, 2019), https://www.bbc.com/news/technology-50048144.

content based on whom the device sees.

For Face Match to work, the Nest Hub Max's camera is designed to be a modern Eye of Sauron—constantly watching and waiting to identify a face it knows. This means the Google device indiscriminately captures the face geometry of any Texan who happens to come into view, including non-users who have never authorized Google to capture their biometric information and who, in all likelihood, may not even know Google is doing so. And, as with Google Photos, this means Google captures the biometric information of Texan children, who may be drawn by curiosity to stand in front of the Nest Hub Max as the camera watches and analyzes them.

But there is more—Google is also listening. Google's Nest line, as well as many other products, comes equipped with Google Assistant, a "voice-controlled personal assistant."[6] Google has programmed Google Assistant into cars, phones, speakers, televisions, laptops, tablets, wearables, displays, thermostats, cameras, doorbells, alarm systems, Yale Locks and more—devices blanketing almost every inch of Texans' homes and personal lives. When activated by a simple "hey Google," Google Assistant records what it hears. In Google's own words, "Google records your voice and audio, plus a few seconds before, when you use audio activations."[7] Upon hearing, recording, obtaining, and analyzing such audio, Google begins to build user profiles and refine how Google Assistant responds. All of these features depend on one critical technological step: Google's ability to capture individuals' unique voiceprints. Just as with Face Grouping and Face Match, Google Assistant's "Voice Match" feature uses voice printing to identify who is speaking to the software.

---

[6] *Use Google Assistant with Nest Products*, GOOGLE NEST HELP (last visited Feb. 13, 2022), https://support.google.com/googlenest/answer/9325085?hl=en.

[7] *Manage Audio Recordings in Your Web & App Activity*, GOOGLE SEARCH HELP (last visited Feb. 13, 2022), https://support.google.com/websearch/answer/6030020?hl=en&co=GENIE.Platform%3DDesktop#zippy=%2Chow-audio-recordings-are-saved.

Said another way, Google uses each voice inflection, mumble, stutter, accent, pattern, and whisper to identify speakers and, through machine learning, to improve Google's products and services. Google does all this by listening to and analyzing every voice it hears, without regard to whether a speaker has consented to Google's indiscriminate voice printing. And perhaps most startling of all, Google has specifically worked on better identifying and differentiating the voices of our children. Accordingly, Google records—without consent—friends, children, grandparents, and guests who stop by, and then stores their voiceprints indefinitely.

Google's all-encompassing effort to use its commercial products to capture biometric identifiers of unwitting Texan users and non-users alike is alarming. It is also unlawful under the Texas Capture or Use of Biometric Identifier Act, which the Texas Legislature specifically designed to protect Texans' privacy by preventing such conduct.

II. 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 nonmonetary relief and claims for monetary relief, including penalties and attorneys' fees and costs in excess of $250,000.

III. PUBLIC INTEREST

2. Plaintiff has reason to believe Defendant has engaged in, and will continue to engage in, the unlawful practices set forth below. Plaintiff has further reason to believe Defendant has caused and will cause adverse effects to users in Texas, to legitimate business enterprises that lawfully conduct trade and commerce in this state, and to the State of Texas. Therefore, the Consumer Protection Division of the Office of the Attorney General of the State of Texas is of the opinion that these proceedings are in the public interest.

IV. JURISDICTION

3. This action is brought by Attorney General KEN PAXTON in the name of the State of Texas and in the public interest under the authority granted him by § 503.001(d) of the Texas Capture or Use of Biometric Identifier Act, TEX. BUS. & COM. CODE ANN. § 503.001 et seq. ("CUBI"), upon the grounds that Defendant has captured Texans' biometric identifiers without consent and/or failed to destroy captured biometric identifiers, as defined in and declared unlawful by subsections 503.001(b), (c)(2), and (c)(3) of the CUBI. In enforcement suits filed pursuant to section 503.001(d) of the CUBI, the Attorney General is further authorized to seek civil penalties of up to $25,000 for each violation.

4. Google has extensive and ongoing business operations throughout Texas, including operations conducted by itself and by various other affiliated entities Google has registered with the State. This has been the case for many years. Google has appeared as a party to many lawsuits in Texas state and federal courts, as both plaintiff and defendant. Google provides products and services to millions of Texans across every corner of the State, has multiple corporate offices in multiple cities in the State, uses the State's residents and resources to test new products and services, such as Google Fiber, and is, therefore, essentially at home in Texas. The allegations herein relate to many, but not all, of Google's overwhelming contacts with the State and arise from Google's conduct vis-à-vis users Google knows to be using Google's products and services in the State. Google is doing business in Texas and is subject to both general and specific personal jurisdiction of this Court. Solely by way of illustrative examples, Google contracts by mail or otherwise with Texas residents and either party is to perform the contract in whole or in part in this state, Google commits torts in whole or in part in this state, and Google recruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside

this state.

V. DEFENDANT

5. Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

6. Google is a technology company that specializes in Internet-related products and services, which include online advertising technologies, search, cloud computing, and other software and hardware.

7. Google markets, advertises, offers, and provides its products and services throughout the United States, and the number of Google's Texas users is likely in the millions.

VI. VENUE

8. Venue of this suit lies in Midland County, Texas pursuant to section 15.002(a) of the Texas Civil Practice and Remedies Code because all or a substantial part of the events or omissions giving rise to these claims occurred in Midland County, Texas.

VII. ACTS OF AGENTS

9. Whenever in this Petition it is alleged that Defendant did any act, it is meant that Defendant performed or participated in the act or Defendant's officers, agents, or employees performed or participated in the act on behalf of and under the authority of the Defendant.

VIII. FACTUAL ALLEGATIONS

A. Uses for Biometric Identifiers Range from Everyday App Access to Targeted Criminal Activity.

10. Biometric data, including fingerprints, face geometry, voice prints, and the like, constitutes immutable characteristics unique to each person. During the recent boom in digital technology, using biometric data to link a person to an activity has become increasingly common. Big Tech companies, like Google, have invested substantial resources to develop efficient ways to identify, link, and leverage biometric data.

11. For example, it is now possible to scan a face (or a photo or video depicting a face) and create a digital map of that face. Once made, the map's data is extracted and analyzed to generate a profile unique to the face that is expressed in a string of data. The ability to distill the unique physical features of a particular face down into data means that facial recognition can be used *with consent* for many everyday activities, such as unlocking phones and accessing password-protected accounts.

12. But the capture and storage of biometric identifiers also present grave risks. For example, stalkers are able to use facial recognition to develop and track their victims. And facial-recognition technology has been widely criticized as inherently biased against women and racial minorities.[8]

13. Criminals benefit from facial recognition in other ways, too. For one thing, faces cannot be encrypted or easily hidden, and Big Tech companies are constantly developing ways to detect and extract data even from faces that are covered, perhaps by a mask. And the power of modern technology means that a criminal can utilize photos of a face taken from long distance or photos of a face that is partially obstructed. Criminals also can simply find and use photos on social-media platforms and other public sources.

14. Criminals can then use images of others' faces to find, steal, and use other data on those individuals, including phone numbers, bank accounts, addresses, relatives, and employment information. Facial recognition thus makes stalking, identity theft, and similar crimes easier.[9]

---

[8] *See e.g.*, Jon Porter, *Federal Study of Top Facial Recognition Algorithms Finds 'Empirical Evidence' of Bias*, VERGE (Dec. 20, 2019, 9:27 AM), https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon.

[9] Taylor Kay Lively, *Facial Recognition in the United States: Privacy Concerns and Legal Developments*, ASIS INT'L (Dec. 1, 2021), https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/.

B. Texas Law Protects Biometric Identifiers.

15. Biometrics is "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity."[10] Biometric data are often used in facial-recognition technology that scans a human face—in person or by photograph—and then extracts data such as face geometry to compare against a database. If the database contains a match, an individual can be identified and the match enhances the database with respect to that individual. This technology is deployed on cell phones and in applications used by Texans on a daily basis, whether the identified individuals realize—let alone consent to—it or not.

16. Biometrics also include voiceprints—*i.e.*, a recording of someone's speech. By analyzing voiceprints for specific data points, high-powered algorithms are able to identify an individual's unique speech pattern and tonality, among other things. As more speech from an individual is captured, analyzed, and grouped with other recordings from the same individual, artificial intelligence ("AI") works in the background and becomes "smarter" at recognizing that individual and develops a more nuanced understanding of voiceprints generally. Big Tech companies, like Google, deploy their advanced AI on voiceprints as just one more way to tailor products to specific users.

17. The intrusiveness of such technology has given rise to widespread privacy concerns. Accordingly, the Texas Legislature passed the CUBI to protect the sanctity of each individual's biometric information.[11] The law reflects Texas's recognition of the deeply

---

[10] *Biometrics*, MERRIAM-WEBSTER (last visited Feb. 11, 2022), https://www.merriam-webster.com/dictionary/biometrics.

[11] George Orwell presciently warned years ago:

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision

sensitive issues surrounding the practice of biometric-data analysis, Texas's commitment to regulating such practices to protect individuals' identity and privacy, and Texas's determination that individuals, not multi-national corporations, should have the final say on how and when their biometric data is collected.

18. The CUBI defines a "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." TEX. BUS. & COM. CODE § 503.001(a). It is unlawful to "capture" an individual's biometric identifier for a commercial purpose unless the individual is informed and consents to having such information collected ***before*** capture. *Id*. at § 503.001(b) (emphasis added). Further, the CUBI mandates that those who are in possession of individuals' biometric identifiers must destroy such information "within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the [biometric] identifier expires." *Id*. at § 503.001(c)(3).

C. Google Captures Texans' Biometric Identifiers Through Google Photos in Violation of the CUBI.

1. Google Captures Texans' Biometric Identifiers from Photographs and Videos Uploaded to Google Photos.

19. Google began offering users the ability to store and share their photos and videos using Google Photos in May 2015. Google Photos is a commercial product that relies on and interacts by default with other Google products, like the Company's Android devices and its cloud-storage services.

20. Since first introduced, Google Photos has used facial-recognition technology, AI, and machine learning to scan photos and videos uploaded by users and automatically group

---

which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment.

GEORGE ORWELL, 1984, at 4 (HBJ Pub. 1977 ed.).

those photos and videos into categories.[12] This technology is capable of identifying faces, recognizing landmarks, and detecting other objects.[13] Upon information and belief, Google's technology is so advanced that, when it captures an individual's facial geometry, Google's AI is able to estimate the individual's mood and sentiments.

21. In fact, since at least May 2015, Google has actively used AI to scan, identify, and organize people depicted in photographs and videos taken on Texans' Android devices or uploaded to Google Photos from either Android or non-Android devices.[14] This feature is referred to as "Face Grouping."

22. Google's Face Grouping uses facial-recognition technology and happens through several steps when a set of photos and/or videos is loaded into Google Photos. First, Google detects whether any photo or video has a face in it. When Google detects a face, it creates a face model or template for that face that establishes a record of an individual's face geometry. Second, Google's algorithmic models evaluate the similarity between various faces to determine whether two images depict the same face. Third, photos and videos that likely depict the same face based on similarities, such as face geometry, are grouped together. On information and belief, the data analyzed and predicted for a given face is as nuanced and as personal as the placement of an individual's eyes, nose, mouth, and even emotional state.[15] Figure 1, below, is an image from Google's online blog demonstrating how Google's Vision API approaches face detection in photography.

---

[12] Ryan Whitman, *The New Google Photos App Will Automatically Group Your Images by Faces and Recognized Objects Like Cars, Skylines, and Food*, ANDROID POLICE (May 25, 2015), https://www.androidpolice.com/2015/05/25/the-new-google-photos-app-will-automatically-group-your-images-by-faces-and-recognized-objects-like-cars-skylines-and-food/.

[13] *Id.*; *see e.g.*, Parth Shah, *How to Improve Facial Recognition in Google Photos*, GUIDING TECH (Aug. 28, 2021), https://www.guidingtech.com/improve-facial-recognition-in-google-photos/.

[14] Whitman, *supra* note 12.

[15] *Detect Faces*, GOOGLE CLOUD (last visited Feb. 11, 2022), https://cloud.google.com/vision/docs/detecting-faces.

Figure 1

23. Google's Vision API is one of the Company's cloud-computing services, and Google claims that "Google Cloud is a suite of cloud computing services that runs on the ***same infrastructure that Google uses internally for their own consumer products***, such as Google Search, Gmail, and YouTube."[16] Accordingly, Figure 1 and Google's descriptions of the infrastructure behind Vision API describes the infrastructure behind its own consumer product, Google Photos—which itself is a cloud-based product.

24. On information and belief, that infrastructure—i.e., the artificial intelligence that powers Google Photos—is FaceNet. As one leading biometrics company explains, FaceNet is the "artificial neural network . . . used in Google Photos to automatically tag photos in which a person's face is recognized."[17] FaceNet has an extremely high accuracy rate" and "uses the 'Labelled Faces in the Wild' dataset which is a public benchmark for facial verification."

[16] *What is Cloud Computing?*, GOOGLE CLOUD (last accessed Feb. 14, 2022), https://cloud.google.com/learn/what-is-cloud-computing (emphasis added).

[17] *How Facial Recognition Works: Technology Explained in Detail*, RecFaces (Oct. 27, 2020), https://recfaces.com/articles/how-facial-recognition-works.

25. On information and belief, the AI and machine learning Google deploys to carry out this process predicts additional attributes, such as age, gender, race, ethnicity, and location.

26. In practical terms, this all means that when a Texan takes a photograph of their family with an Android device or uploads a photograph of their family to Google Photos, Google uses facial-recognition technology to (i) scan the photograph for facial geometry and other biometric identifiers, (ii) compare the newly uploaded facial geometry and biometric identifiers to the data previously captured and stored by Google to attempt to identify similarities; (iii) identify each family member based on the collected biometric identifiers, and (iv) create photo albums sorted by the unique facial structures of each family member.

27. As noted, when Google Photos detects a face, it generates a face template, or a face model, of that face. Buried deep on one of its support pages, for example, Google states that disabling face grouping deletes the "[f]ace models used to create those face groups."[18]

28. Google Photos does not stop with analyzing just photos. Google Photos also detects, analyzes, and groups faces identified in videos. In fact, Google seemingly admits to this by explaining to users how to "search using suggestions" for "People & Pets: all of the photos and videos of your close ties."[19] Even further, Google owns a portfolio of patents relating to facial recognition for videos.[20] Notably, under Google's "learn about face models" support information, Google does not mention using face models for faces detected in videos.[21]

---

[18] *Search by People, Things & Places in Your Photos*, GOOGLE PHOTOS HELP (last visited Feb. 20, 2022), https://support.google.com/photos/answer/6128838?hl=en&ref_topic=6128818#nofacegrouping.

[19] *Search by People, Things & Places in Your Photos*, GOOGLE PHOTOS HELP (last visited Feb. 17, 2022), https://support.google.com/photos/answer/6128838?hl=en&co=GENIE.Platform=Android.

[20] *E.g.*, U.S. Patent No. 9,984,729 (filed Feb. 1, 2016); U.S. Patent No. 8,457,367 (filed June 26, 2012); U.S. Patent No. 8,213,689 (filed July 14, 2008); U.S. Patent No. 6,301,370 (filed Dec. 4, 1998).

[21] *Search by People, Things & Places in Your Photos*, GOOGLE PHOTOS HELP (last visited Feb. 20, 2022), https://support.google.com/photos/answer/6128838?hl=en&ref_topic=6128818#nofacegrouping.

29. The information Google collects during the grouping process is used to create and store templates of individuals' faces—for both users and non-users alike. As users take additional photos and videos on their Android devices or upload additional photos and videos to Google Photos, Google's technology continues the grouping process.

30. On information and belief, the more users save photos and videos to the cloud-based Google Photos, the more advanced Google's technology and artificial-intelligence capabilities become because of Google's machine-learning methods. In other words, the more photos and videos Google's technology processes and the more faces the technology analyzes, the better the technology becomes at predicting and grouping attributes in future photos and videos. This means the process Google uses for Face Grouping helps Google stay ahead of its competitors in the marketplace; and, as Google's photos app becomes more advanced, more users upload more photos and videos, leading to a snowball effect of more users purchasing more storage on Google's cloud services.

31. Google's commercial use of this process is not immaterial. Indeed, after years of offering free photo storage, Google now charges for that service. As described by Bloomberg in late 2020, "Google said it will start counting new uploads to Google Photos against each user's cap of 15 gigabytes of free storage with the company, starting next June. Once you hit that limit, you'll have to start paying $1.99 a month to up your storage space (unless you're using a Google Pixel phone). It may seem like an insignificant amount, but it could generate as much as $3 billion a year in new revenue for Google's parent company, Alphabet Inc., by 2023, estimates Bernstein analyst Mark Shmulik."[22]

[22] Gerrit De Vynck, *Google is Going to Start Cashing in on Your Old Photos*, BLOOMBERG (Nov. 13, 2020, 5:45 AM) https://www.bloomberg.com/news/newsletters/2020-11-13/google-is-going-to-start-cashing-in-on-your-old-photos.

32. On information and belief, Google does not destroy the biometric identifiers it captures through Google Photos before the first anniversary of the date the purpose for collecting the identifiers expires.

2. Google Does Not Inform or Obtain Consent from Texans Prior to Collecting Biometric Identifiers.

33. Google Photos comes pre-installed on all Android devices. Similarly, Google Photos is available on the Apple App Store and can be installed on Apple devices. Despite the sophistication of Google's facial-recognition technology, as described above, the technology does not distinguish between Google Photos users and non-users. Further, on information and belief, at no point does Google affirmatively inform users, much less non-users, that records of their biometric identifiers are being captured and stored. Nor does Google affirmatively obtain consent to capture and store records of biometric identifiers from users or non-users who appear in photos and videos uploaded to Google Photos. Nor does Google inform users or non-users that the records are stored for more than one year.

34. Google's Face Grouping feature, which scans, processes, and indexes biometric data taken from photographs and videos of both users and non-users, makes Google's actions even more troubling. In such a scenario, Google cannot possibly have obtained all individuals' consent before capturing their biometric identifiers. And, on information and belief, Google does this even for photos and videos depicting minor children. Regardless, Google still employs the Face Group feature.

35. Further, Google Photos users are not afforded an opportunity to opt out of Google's Face Grouping feature until after the user uploads at least one photo or video into Google Photos, at which point Google has already scanned and extracted biometric identifiers from the

photo or video.[23] Ultimately, these processes result in the capture of biometric information of unwitting users and non-users, including minors and other individuals whom Google has failed to inform of Google's practices and whom may be unable to provide the requisite consent.

D. Google Captures Texans' Biometric Identifiers Through Google Nest Devices in Violation of the CUBI.

1. The Nest Hub Max Indiscriminately Captures the Face Geometry of Non-Consenting Texan Passersby.

36. One of Google's popular smart-home commercial products is the Google Nest, previously known as Google Home. The Nest Hub Max is a Google device sold in Texas and to Texans that comes equipped with speakers, a microphone, a camera, and a touchscreen display that somewhat resembles a tablet. Google advertises the Nest Hub Max as a tool to "help[] your busy family stay in touch and on track" with features that allow users to "[l]eave video messages and make video calls;" "[c]heck in on home when you're away with the built-in Nest Cam;" and "[s]hare reminders and to-dos."[24]

37. The Nest Hub Max includes a feature Google calls "Face Match." As Google describes it, Face Match is a facial-recognition tool designed "to provide a proactive experience that's tailored to each user." Face Match does this when Google "recognizes your face" and thereafter "show[s] you your personalized content," such as "video messages, reminders, and upcoming calendar events."[25]

---

[23] It is unclear from Google's documentation whether Google prevents a user who "opts out" from then having their biometrics captured when they are a third party in another user's photos or video, but the failure to do so would also violate CUBI .

[24] *Introducing Google Nest Hub Max*, GOOGLE NEST HELP (last visited Feb. 14, 2022), https://support.google.com/googlenest/answer/9334359?hl=en.

[25] *Face Match on Google Nest Hub Max*, GOOGLE NEST HELP (last visited Feb. 14, 2022), https://support.google.com/googlenest/answer/9320885?hl=en&ref_topic=7029677.

38. To enable Face Match, a user must use their device to scan their face, which allows Google to create and store a face template for that individual user. This process can be done for multiple users, allowing the Nest Hub Max to identify various household members as they are using the device and to provide user-specific content.

39. Public reporting has revealed that, when the Face Match feature is on, the Nest Hub Max's camera is always on and constantly scanning for a face it recognizes.[26] On information and belief, the Nest Hub Max does not require a screen touch or any other prompt for the camera to begin scanning for faces and instead is constantly scanning as long as the Face Match feature is on.

40. On information and belief, the "always-on" feature of Face Match means that every time Google's Nest Hub Max detects a face within the camera's view , Google scans and records the face geometry of the face it detects for comparison against the device's database of user faces. This means the Nest Hub Max can quickly identify if it is viewing the face of a registered user, at which point the device can populate the appropriate content for that user.

41. On information and belief, however, the always-on feature also means that any time a non-user appears in view of the Next Hub Max camera Google scans and records the face geometry of that non-user for comparison against the device's database of faces. Such scanning and recording takes place irrespective of whether such a non-user is aware of—let alone consents to—the scanning and recording of the non-user's face. And then, Google consequently records the face geometry of minor children who come into view of the Nest Hub Max's camera.

[26] Dale Smith, *Google Knows What You Look Like. Here's What it Means and How to Opt Out*, CNET (Feb. 4, 2020, 5:00 AM) https://www.cnet.com/home/smart-home/google-knows-what-you-look-like-heres-what-it-means-and-how-to-opt-out/.

42. Additionally, with a Nest Aware subscription, "[w]hen your camera detects a face, it creates a 'faceprint' (biometric signature) to compare with other faces in the library."[27]

43. On information and belief, the Nest Hub Max periodically sends the records of face geometry saved on a given device to the cloud. Google captures and uses this biometric data for the commercial purpose of, among other things, improving product experience.[28] Google states on its support page for Nest's people-detection feature, for example, that certain "kinds of improvements require a lot of computing power, much more than your Nest camera or doorbell can deliver by itself. So we use powerful cloud servers to make Nest Aware's state-of-the-art detection possible, and we're constantly improving the algorithms to provide the best possible experience."[29] Further, data is shared among devices: "All your cameras in the same home share the same familiar face library. If you add a new camera to the same home, it uses the same familiar face library as the other cameras in your home, so you don't have to teach it as much."[30]

44. On information and belief, Google does not destroy the biometric identifiers it captures through the Nest Hub Max tools and features before the first anniversary of the date the purpose for collecting the identifiers expires.

2. Google's Nest Devices and Google Assistant Indiscriminately Capture Biometric Data of Non-Consenting Texans.

45. Google does not stop with facial recognition. Google's suite of Nest products and other Google hardware utilize Google Assistant, which records, stores, and analyzes voiceprints.

---

[27] *How Nest Cameras Detect Sound and Motion*, GOOGLE NEST HELP (last visited Feb. 18, 2022), https://support.google.com/googlenest/answer/9250426#zippy=%2Cfamiliar-face-detection.

[28] *Id.*

[29] *Learn About Nest Sense*, GOOGLE NEST HELP (last accessed Feb. 18, 2022) https://support.google.com/googlenest/answer/9274904?hl=en&ref_topic=9360834#zippy=%2Cnest-cameras-and-doorbells.

[30] *Familiar Face Detection*, GOOGLE NEST HELP (last accessed Feb. 18, 2022), https://support.google.com/googlenest/answer/9268625.

Google uses a setting called Voice & Audio Activity to record voices and audio and to improve the Company's speech-recognition capabilities.

46. Google Nest is Google's commercial line of smart-home products, which include cars, wearables, speakers, displays, cameras, doorbells, locks, thermostats, and alarm systems. Embedded in these products is Google Assistant, a voice-activated system endorsed as a user's "personal assistant."

47. Users activate Google Assistant by saying a short command, such as "hey Google" or "okay Google." From there, Google Assistant can do anything from dimming lights and finding recipes to creating to-do lists and engaging cameras.[31]

48. In order to respond to commands that could come at any time, Google Assistant must be—and is—always listening. When activated by the relevant command, Google Assistant begins recording the voices and speech it hears. Google Assistant also reaches back and captures the three seconds of sound it heard *before* receiving the activation command. After collecting all this data, Google then stores these recordings.[32]

49. Google uses the stored audio files to build and fine-tune voice profiles on each individual whose voice Google has recorded. Google does this profiling with AI and, upon information and belief, by employees who physically listen to files.[33] In fact, Google tasked these employees and subcontractors with more than merely listening to voice recordings captured by Google Assistant. Google asked the employees and subcontractors to search words, addresses, names, company names, and other personal information discussed in the

[31] *Overview*, HEY GOOGLE (last visited Feb. 13, 2022), https://assistant.google.com/.
[32] *See e.g.*, Michael Timmermann, *Google is Recording Your Voice: How to Listen to (and Delete) the Files,* CLARK.COM (Oct. 26, 2017), https://clark.com/technology/google-recording-you-delete-files/.
[33] Tim Verheyden et al., *Google Employees Are Eavesdropping, Even in Your Living Room, VRT NWS Has Discovered*, VRT NWS (Jul. 10, 2019, 4:39 PM), https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/.

recordings, with the practical effect of potentially revealing the personal identity of certain speakers.[34] Google attempted to minimize the magnitude of intrusion by confirming to public news sources that only 0.2% of all audio clips collected by Google Assistant were subjected to human review.[35] But, given the billion Google Assistant users,[36] Google employees or subcontractors may have reviewed millions of recordings made by unsuspecting individuals speaking near a device with Google Assistant. In other words, Google had human beings listen to the most intimate conversations about everything that people discuss in the safety of their own home including sex, religion, politics, and health.

50. When activated, Google Assistant begins recording and storing voiceprints for every voice it can detect. Just as Google employs Face Match to scan and identify the faces of the Texans who appear before Google's cameras, the Company employs "Voice Match" to print the voice of any Texas that speaks within "earshot" of Google Assistant. This is necessary for Assistant to determine whether it is listening to a known user as well as *which* known user, since Google Assistant is able to use its neural network to support multiple users.

51. There are at least three categories of individuals whose voice Google records. First, there are owner-users, who may own a device or live in the household with the device, have some minimal understanding of how the product works, and intentionally engage Google Assistant with their voice commands. Second, there are non-owner users, who may visit a household with a device with Google Assistant and engage the product without fully

[34] Gabriela Galindo, *Google Listens to Conversations Recorded by Its Smart Home Devices*, BRUSSELS TIMES (Jul. 11, 2019), https://www.brusselstimes.com/news/belgium-all-news/60444/google-listens-to-conversations-recorded-by-its-smart-home-devices.
[35] *Id*.
[36] Richard Nieva, *Google Assistant Now Has 500 Million Monthly Users*, CNET (Jan. 7, 2020, 10:00 AM), https://www.cnet.com/tech/tech-industry/google-assistant-now-has-500-million-monthly-users/.

knowing or understanding or consenting to how the product works, what privacy controls are available, or what privacy settings are activated. Finally, there are non-users who may be speaking in the background when Google Assistant is activated and who did not consent to Google recording their voice.

52. When Google Assistant records and analyzes the detected voices, Google Assistant does not differentiate between owner-users, non-owner users, and non-users. On information and belief, Google Assistant instead records every voice it detects and creates voiceprints for each individual the device hears. Indeed, in or around early 2019, Google confronted the problem in connection with its "Assistant for Kids" project that Google Assistant's voice-recognition technology sometimes was unable to differentiate between children because of their similar-sounding voices—a problem that could only be encountered because Assistant was capturing the voiceprints of every child it heard, regardless of whether the child had consented to Google capturing their biometric information.

53. Accordingly, Google Assistant records and creates voiceprints for individuals who did not—and have no means to—consent to the recording. Further, Google used an "opt-out" system for storing voiceprints until August 2020, meaning that Google's settings were defaulted to store voiceprints until that time.[37]

54. By way of example, if a parent, who is an owner-user, activates Google Assistant to look up a cocktail recipe while hosting family friends, Google Assistant will begin recording every voice it detects until its task is completed. If the family friends are speaking to the parent's four-year-old son, Google Assistant will capture and create voiceprints for the

[37] Jules Want, *Google Opts Out All Users of Voice Data Collection, Explains What it Does with the Data,* ANDROID POLICE (Aug. 6, 2020), https://www.androidpolice.com/2020/08/06/google-opts-all-users-out-of-voice-data-collection-explains-what-it-does-with-the-data/.

family friends and the four-year old. Those individuals did not—and could not—consent to Google's voice printing.

55. For this very reason, Google Senior Vice President for Hardware admitted to the BBC in 2019 that Google "products themselves should try to indicate" to a Nest owner's guests that a Nest is present in the home so that guests are aware that their voices may be recorded.[38] Yet, Google continues to record and voiceprint the voices of children and other non-owners without indicating that this is happening.

56. Not only does analyzing voiceprints allow Google to personalize Google Assistant's responses, but Google also admits to using the data to improve Google's own AI.[39] Given that Google uses voice assistance and recognition for Google Search, Google Assistant, and Google Maps, among other products, the collection and analysis of troves of voice data and human-speech patterns provide a powerful means for Google to enhance its product offerings and capabilities, which ultimately translates into market dominance and increased profits.

57. On information and belief, Google does not destroy the biometric identifiers it captures through Google Assistant before the first anniversary of the date the purpose for collecting the identifiers expires. In fact, in certain cases, users must manually delete recordings of their own voices, assuming a user even knows Google has stored such recordings.[40] And, if a user chooses to allow Google to store the recordings, Google can ultimately store the

---

[38] Leo Kelion, *Google Chief: I'd Disclose Smart Speakers before Guests Enter My Home,* BBC NEWS (Oct. 15, 2019), https://www.bbc.com/news/technology-50048144.

[39] *Manage Audio Recordings in Your Web & App Activity*, GOOGLE ACCOUNT HELP (last visited Feb. 14, 2022), https://support.google.com/accounts/answer/6030020?hl=en&co=GENIE.Platform%3DDesktop#zippy=%2Cdelete-recordings-from-your-web-app-activity ("Your audio can help Google develop and improve its audio recognition technologies and the Google services that use them.").

[40] *Id.*; *Delete Your Activity,* GOOGLE ACCOUNT HELP (last visited Feb. 14, 2022), https://support.google.com/accounts/answer/465.

recordings indefinitely. This means that, in some circumstances, Google holds the biometric identifiers of non-owner users and non-users indefinitely without the non-owner user or non-user ever knowing Google captured their biometric identifiers in the first place.

58. Further, owners of Nest products may subscribe to a Google service called "Nest Aware."[41] For a fee, Nest owners can unlock additional Nest product features, which include a longer retention period for videos captured by Nest devices and an intelligent-alert feature called "familiar faces." The familiar faces feature detects and learns the faces of individuals appearing in videos captured for Nest Aware subscribers. Google's AI analyzes the faces detected in these videos and, if the face is recognized, groups together previous clips containing that individual's face. These clips are stored and can be reviewed by the Nest Aware subscriber.

59. Google acknowledges that it does not inform or obtain consent from non-subscribing individuals whose face geometry, voiceprint, and other biometric identifiers may be captured and stored for Nest Aware subscribers.[42]

60. Google's Nest product line is just one representative example of how Google Assistant captures the facial geometry and voiceprints of non-consenting individuals. Google Assistant indiscriminately captures the voiceprints of all detectable voices on all devices that employ the Google Assistant technology, including at least cars, phones, speakers, televisions, laptops, tablets, wearables, displays, thermostats, cameras, doorbells, alarm systems, and more devices.[43]

---

[41] *Nest Aware*, GOOGLE STORE (last visited Feb. 14, 2022), https://store.google.com/us/product/nest_aware?hl=en-US.

[42] *Nest Terms of Service*, PROD. DOCUMENTATION HELP (last visited Feb. 14, 2022), https://support.google.com/product-documentation/answer/9327735?hl=en.

[43] *Google Assistant Now in Even More Devices*, HEY GOOGLE (last visited Feb. 14, 2022), https://assistant.google.com/platforms/devices/.

E. Google Captures Texans' Biometric Identifiers for Commercial Purposes.

61. Google captures Texans' biometric identifiers for commercial purposes. As discussed above, Google commercializes its so-called "free" programs by ensuring that Texans must ultimately pay for storing their data—such as photos and videos on Google Photos.

62. Additionally, Google sells Nest owners the Nest Aware service, which includes the "familiar faces" feature. Google profits through its Nest Aware service by, among other things, capturing, storing, and analyzing the face geometry, voiceprint, and other biometric identifiers of non-consenting individuals.

63. Additionally, Google's primary business is collecting and mining troves of user data. Through its many commercial products and services, Google analyzes this data to support its digital advertising business. On information and belief, Google Photos operates to enrich the data points Google collects on individuals, enabling the Company to increase its already massive advertising revenues.[44] Ultimately, Google has turned Texans' desire to take, store, and share photos and videos into a testing ground for AI and other products in its ever-growing, advertising-revenue stream. And, Google has enlisted the friends and family members of those Texans as non-consenting, unknowing participants in Google's scheme.

64. Other commercial purposes for which Google captures Texans' biometric identifiers include improving Google's other AI, services, and hardware. As noted above, each time Google's algorithms process photos and videos to detect certain faces and objects or process voiceprints to better understand voice data, Google's underlying AI becomes stronger, better-informed, more efficient, and more dominant. This translates into

[44] Marty Swant, *Google Reports Strong Third-Quarter Advertising Revenue, Shrugging Off Apple Privacy Changes*, FORBES (Oct. 26, 2021, 9:05 PM), https://www.forbes.com/sites/martyswant/2021/10/26/google-reports-strong-third-quarter-advertising-revenue-shrugging-off-apple-privacy-changes/?sh=302c1ee52f43.

commercial benefits for Google through both increased revenue and the ability to refine and market application programing interfaces ("APIs") to developers.

65. As to hardware, Google similarly converts trained AI into improved hardware. For example, as Google processes massive data sets of photographs and videos, Google obtains insights that inform the design of the cameras Google will place on its phones. Google also has historically driven the sales of its Pixel phones by granting certain Pixel users "free" Google Photos storage and others a "Pixel Pass" granting 200GB of storage—further crystallizing the nexus between Google software and hardware.[45]

IX. CAUSES OF ACTION

Count I
Violations of the Texas Capture or Use of Biometric Identifier Act
TEX. BUS. & COM. CODE ANN. § 503.001 (b)&(c) et seq.

66. Defendant, as alleged above, repeatedly captured and possessed biometric identifiers of unsuspecting Texans each time a photo or video was taken on an Android device or otherwise uploaded to Google Photos and then processed by Google's face-grouping processes, which recorded individuals' biometric information, including individuals' face geometry.

67. Defendant is a Delaware corporation and is a "person" under CUBI.

68. CUBI expressly defines "biometric identifier" to include a "record of hand or face geometry" and a "voiceprint."

69. Since at least 2015, Defendant captured and possessed Texans' biometric identifiers for a commercial purpose without informing and obtaining consent from individuals prior to capturing such information in violation of Texas Business and Commerce Code

[45] Jonathan Lamont, *These Google Pixel Phones Will Still Get Free Photos Backups after June 1*, MOBILE SYRUP (May 26, 2021, 3:08 PM), https://mobilesyrup.com/2021/05/26/google-pixel-phones-free-backups-photos-june-1/.

§ 503.001(b) by:

A. Configuring Google Photos (including related programs using Google APIs) to automatically capture and possess records of individuals' face geometry using facial recognition software;

B. Failing to inform and obtain consent from users and non-users of Google Photos of this default setting and the implications of thereafter allowing Google to capture records of face geometry from that photo or video;

C. Allowing Google Photos users to disable this facial recognition software only after uploading a photo or video and having allowed the photo or video to be scanned by the same facial recognition software; and

D. Using the captured records of face geometry for a commercial purpose, namely, to:

i. improve Google's advertising and subscription revenues;

ii. develop the efficiency and capabilities of Google's AI and machine-learning; and

iii. carry out functions and features designed to keep Google's products and brand competitive in the marketplace.

70. Defendant further captured and possessed Texans' biometric identifiers for a commercial purpose without informing and obtaining consent from individuals prior to capturing such information in violation of Texas Business and Commerce Code § 503.001(b) by:

A. Configuring the Google Nest Hub Max and related Google hardware devices to automatically and indiscriminately capture records of individuals' face geometry using facial-recognition technology;

B. Failing to inform and obtain consent from individuals whose records of face geometry were captured by Google that the Google Nest Hub Max and related Google hardware devices could be actively looking to capture the face geometry of any and every face that come into a camera's field of vision; and

C. Using the captured biometric identifiers for a commercial purpose, namely, to:

i. improve Google's advertising and subscription revenues;

ii. develop the efficiency and capabilities of Google's AI and machine-learning; and

iii. carry out functions and features designed to keep Google's products and brand competitive in the marketplace and/or directly generate subscription revenue, such as Google's Nest Aware paid-subscription service.

71. Defendant further captured Texans' biometric identifiers for a commercial purpose without informing and obtaining consent from individuals prior to capturing such information in violation of Texas Business and Commerce Code § 503.001(b) by:

A. Configuring Google Assistant to record voiceprints of device owner-users without the device owner's consent;

B. Configuring Google Assistant to record voiceprints of non-owner users without the non-owner user's consent;

C. Configuring Google Assistant to record voiceprints of non-users without the non-user's consent;

D. Recording voiceprints from before a user voice-activates Google Assistant; and

E. Using the captured biometric identifiers for a commercial purpose, namely, to:

i. improve Google's advertising and subscription revenues;

ii. develop the efficiency and capabilities of Google's AI and machine-learning; and

iii. carry out functions and features designed to keep Google's products and brand competitive in the marketplace and/or directly generate subscription revenue, such as Google's Nest Aware paid-subscription service or its Google Cloud Storage rate plans.

72. Defendant also failed to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which Defendant stores, transmits, and protects any other confidential information Defendant possesses in violation of Texas Business and Commerce Code § 503.001(c)(2).

73. Defendant also failed to destroy the biometric identifiers it captured within a reasonable time period, or before the first anniversary of the date the purpose for collecting the identifier expired, in violation of Texas Business and Commerce Code § 503.001(c)(3).

X. TRIAL BY JURY

74. The State of Texas herein requests a jury trial and will tender the jury fee to the County District Clerk's office pursuant to Texas Rule of Civil Procedure. 216 and Texas Government Code Ann. § 51.604.

XI. PRAYER FOR RELIEF

75. The State further prays that Defendant be cited according to the law to appear and answer herein; that after due notice and a hearing a TEMPORARY INJUNCTION be issued; and upon final hearing a PERMANENT INJUNCTION be issued restraining and enjoining Defendant, Defendant's officers, agents, servants, employees, and attorneys, and any other person in active concert or participation with Defendant from violating the CUBI, including

by enjoining Defendant 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 voice or facial recognition in Texas without the informed consent of all individuals subject to Google's facial-recognition and voice-recognition technology;

C. Failing to destroy the biometric identifiers it captured within a reasonable time period, or before the first anniversary of the date the purpose for collecting the identifier expired; and

D. Misrepresenting, directly and/or by omission, that Google does not collect biometric identifiers.

76. The State further respectfully prays that this Court will:

A. Adjudge against Defendant civil penalties in favor of the State in the amount of not more than $25,000 per violation of the CUBI;

B. Order Defendant to pay the State's attorney fees and costs of court pursuant to Texas Government Code § 402.006(c);

C. Order Defendant to pay both pre-judgment and post judgment interest on all monetary awards as provided by law.

77. The State further prays that this court grant all other relief to which the State may show itself entitled.

Respectfully submitted,

NORTON ROSE FULBRIGHT US LLP

/s/ Marc B. Collier
Marc B. Collier
Texas State Bar No. 00792418
Marc.collier@nortonrosefulbright.com
Julie Searle
Texas State Bar No. 24037162
Julie.Searle@nortonrosefulbright.com
Chris Cooke
Texas State Bar No. 24129241
Christopher.cooke@nortonrosefulbright.com
Chase Sippel
Texas State Bar No: 24126753
Chase.sippel@nortonrosefulbright.com
98 San Jacinto Blvd., Suite 1100
Austin, Texas 78701
(512) 474-5201 – Tel
(512) 536-4598 – Fax

Vic Domen
Vic.domen@nortonrosefulbright.com
(pro hac to be sought)
799 9th Street NW, Suite 1000
Washington, DC, 20001
(202) 662-0200 – Tel

NORTON ROSE FULBRIGHT US LLP

/s/ Joseph M. Graham, Jr.
Joseph M. Graham, Jr.
Texas State Bar No. 24044814
Joseph.graham@nortonrosefulbright.com
Barbara Light
Texas State Bar No. 24109472
Barbara.light@nortonrosefulbright.com
Zachery Newton
State Bar No. 24126971
zachery.newton@nortonrosefulbright.com
Lilly MacDonald
State Bar No. 24126136
lilly.macdonald@nortonrosefulbright.com
Gary Y. Gould
State Bar No. 24104995
gary.gould@nortonrosefulbright.com
Fulbright Tower
1301 McKinney, Suite 5100
Houston, Texas 77010-3095
(713) 651-5151 – Tel
(713) 651-5246 – Fax

/s/ Bradley H. Bains
Bradley H. Bains
State Bar No. 01553080
bbains@cbtd.com
Matt Catalano
State Bar No. 24003918
mcatalano@cbtd.com
COTTON, BLEDSOE, TIGHE & DAWSON, P.C.
P. O. Box 2776
Midland, Texas 79702-2776
432-684-5782
432-682-3672 Fax

KEN PAXTON
Attorney General

/s/ Shawn E. Cowles

Brent Webster, First Assistant Attorney General of Texas
Brent.Webster@oag.texas.gov
Grant Dorfman, Deputy First Assistant Attorney General
Grant.Dorfman@oag.texas.gov
Aaron Reitz, Deputy Attorney General For Legal Strategy
Aaron.Reitz@oag.texas.gov
Shawn E. Cowles, Deputy Attorney General for Civil Litigation
Shawn.Cowles@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
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
Wade Johnson, Assistant Attorney General,
Consumer Protection Division
Wade.Johnson@oag.texas.gov
Lucas Wollenzien, Assistant Attorney General,
Consumer Protection Division
Lucas.Wollenzien@oag.texas.gov
Norman Cahn, Assistant Attorney General,
Consumer Protection Division
Norman.Cahn@oag.texas.gov

OFFICE OF THE ATTORNEY GENERAL OF TEXAS
P.O. Box 12548
Austin, TX 78711-2548
(512) 936-1674

Attorneys for Plaintiff State of Texas