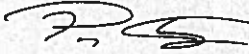


KIRKLAND & ELLIS LLP

MEMORANDUM

TO: Clearview AI, Inc.

FROM: Paul D. Clement, Esq. 

DATE: August 14, 2019

RE: Legal Implications of Clearview Technology

Clearview is an investigative application that uses state-of-the-art facial-recognition technology to match the face in a user-uploaded image to faces in publicly available images. It is designed to be used in ways that ultimately reduce crime, fraud, and risk in order to make communities safer. This memorandum analyzes the potential legal implications of Clearview's use by public entities as an investigative tool. We conclude, based on our understanding of the product, that law enforcement agencies do not violate the federal Constitution or relevant existing state biometric and privacy laws when using Clearview for its intended purpose. Moreover, when employed as intended, Clearview's effective and evenhanded facial-recognition technology promotes constitutional values in a manner superior to many traditional identification techniques and competing technologies.

CLEARVIEW AI TECHNOLOGY

In the simplest terms, Clearview acts as a search engine of publicly available images. Similar to Google, which pulls and compiles publicly available data from across the Internet into an easily searchable universe, Clearview pulls and compiles publicly available images from across the Internet into a proprietary image database to be used in combination with Clearview's facial recognition technology.

Clearview employs state-of-the-art, proprietary facial-recognition technology to match the face that appears in a user-uploaded image with those that appear in Clearview's database of publicly available images. Our technical understanding of this proprietary technology as it relates to matters such as the company's data collection methodologies and facial-recognition algorithms is based on discussions with the company and its senior executives. When a Clearview user uploads an image, Clearview's proprietary technology processes the image and returns links to publicly available images that match the person pictured in the uploaded image. Clearview does not itself create any images, and it does not collect images from any private, secure, or proprietary sources. Clearview links only to images collected from public-facing sources on the Internet, including images from public social media, news media, public employment and educational websites, and other public sources. Frequently, the linked websites containing the matched image include additional publicly available information about the person identified in the matched images. Clicking on a matched image will send the user to the linked external website, outside the Clearview application.

KIRKLAND & ELLIS LLP

Clearview is intended to be used by public entities for a variety of purposes. Clearview can be used as an additional investigative tool to aid public officials, much in the way a Google search can be used to generate and pursue investigative leads. The results from a Clearview search are not intended or designed to be used as evidence in court, whether for purposes of demonstrating probable cause to obtain a warrant or otherwise. A Clearview search is the beginning, not the end, of an identification process. Two recent examples are instructive. In September 2018, a newspaper published a photograph of an unknown suspect who had allegedly assaulted two individuals outside a bar in Brooklyn, New York. Clearview technology compared the suspect's image against its database of publicly available images and returned an identity for the individual based on that publicly available information. This information was conveyed to the police, who subsequently used more traditional investigative tools to confirm his identity. Similarly, in December 2018, a newspaper published a photograph of a man who had allegedly fondled a woman on the New York City subway. Clearview technology matched the photograph to images in its database, and that information was used by the police to identify and apprehend the man.

At present, more than 200 law enforcement agencies across the nation use Clearview technology as part of their arsenal of investigative techniques. Clearview has helped law enforcement identify potential suspects involved in a wide variety of crimes including child exploitation, human trafficking, sexual assault, theft, narcotics, and bank fraud.

LEGAL ANALYSIS

I. Law Enforcement Agencies' Use of Clearview For Its Intended Purpose Is Constitutionally Permissible And Consistent With Existing Biometric And Privacy Laws.

Critics of facial-recognition technology frequently assert, without elaboration, that the use of such technology by law enforcement raises serious legal issues under the federal Constitution and state biometric and privacy laws. An informed legal analysis, however, establishes that law enforcement agencies' use of Clearview for its intended purpose is fully consistent with current federal law and state biometric and privacy laws.

A. Law Enforcement Agencies' Use of Clearview For Its Intended Purpose is Consistent with the U.S. Constitution.

Opponents of facial-recognition technology frequently invoke the Fourth Amendment as a legal barrier to the use of such technology by the government. The Fourth Amendment provides in full: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the Supreme Court recently reaffirmed, the "basic purpose" of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). In particular, the Fourth Amendment "protect[s] certain expectations of privacy" such that, "[w]hen an individual 'seeks to preserve something as

KIRKLAND & ELLIS LLP

private,’ and his expectation of privacy is ‘one that society is prepared to recognize as reasonable,’” the government’s “intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.” *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

The starting point for any Fourth Amendment inquiry, therefore, is whether an individual has an “expectation of privacy” that “society is prepared to recognize as reasonable.” If not, then Fourth Amendment safeguards do not attach. In a series of cases, the Supreme Court has “drawn a line between what a person keeps to himself and what he shares with others.” *Id.* at 2216. A person “has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). That remains true “even if the information is revealed on the assumption that it will be used only for a limited purpose.” *United States v. Miller*, 425 U.S. 435, 443 (1976). The government “is typically free to obtain such information ... without triggering Fourth Amendment protections.” *Carpenter*, 138 S. Ct. at 2216.

Under the foregoing principles, law enforcement agencies’ use of Clearview as intended does not, in our view, “trigger[] Fourth Amendment protections.” When a user uploads an image for matching, Clearview compares that image against *publicly available* images from *publicly available* internet sources—social media, news media, employment networking sites, and so forth. Individuals do not have a reasonable expectation of privacy in images or other information that they (or others) have “voluntarily turn[ed] over to third parties” like social media sites or directly transmitted into the public sphere. *Smith*, 442 U.S. at 734-44; *see also California v. Greenwood*, 486 U.S. 35, 40-41 (1988) (no Fourth Amendment interest in trash placed at a curb for pickup; individuals had put out garbage “for the express purpose of conveying it to a third party” and for, “in a manner of speaking ... public consumption”). That is so even if an individual uploaded an image for a “limited purpose” (for example, a job networking site). *Miller*, 425 U.S. at 443. Just as the Fourth Amendment would not be implicated by using a Google search to obtain information made available on the internet, so too is the Fourth Amendment not implicated by using Clearview to do the same. *See, e.g., Burke v. New Mexico*, 2018 WL 2134030, at *5-6 (observing that “[c]ourts routinely have found that there is no right to privacy in internet postings that are publicly accessible,” and collecting other cases); *United States v. Meregildo*, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (“When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment.”); *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (holding that individual had no reasonable expectation of privacy in files on computer shared over a peer-to-peer file sharing network).

To be sure, the Supreme Court observed in *Carpenter* that “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.” 138 S. Ct. at 2217. The Court held in that case that the Fourth Amendment *is* implicated when the government obtains cell phone records indicating an individual’s physical location, notwithstanding that the location information was arguably “shared” by the user with the cell phone company, thereby removing it from the realm of Fourth Amendment protection. But *Carpenter* was a “narrow” decision that focused on one particular set of circumstances—obtaining cell phone records that provide a “comprehensive chronicle of the user’s past movements.” *Id.* at 2211, 2220. The fact that the technology (and records capturing that technology) created an “exhaustive chronicle” of a person’s “physical movements” was particularly troubling to the Court. *See id.* at 2217 (observing that

KIRKLAND & ELLIS LLP

“individuals have a reasonable expectation of privacy in the whole of their physical movements”); *id.* at 2218 (explaining that the case involved “attempts to reconstruct a person’s movements”); *id.* at 2220 (noting “the unique nature of cell phone location information”). Moreover, the Court emphasized that the cell phone location information both was incidentally generated (rather than voluntarily posted) and was available only to the cell phone provider and not accessible by third parties. The Court explained that cell phone location information “is not truly ‘shared’ as one normally understands the term,” because “a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.” *Id.* at 2220.

None of these concerns is implicated in the case of Clearview: it does not track a person’s “physical movements”; the images against which it compares a user-generated image are made publicly available to a range of third parties by voluntary acts rather than the incidental operation of a device used for other purposes. Indeed, the Court expressly stated in *Carpenter* that it was not “call[ing] into question conventional surveillance techniques and tools, such as security cameras,” or “address[ing] other business records that might incidentally reveal location information.” *Id.* Accordingly, we think it very unlikely that any court would consider Clearview’s use by law enforcement agencies problematic in light of *Carpenter*. To the contrary, the fact that four Justices did not think there was a Fourth Amendment problem in *Carpenter* goes a long way to underscoring the absence of a serious Fourth Amendment problem with the use of Clearview (or Google, for that matter) by law enforcement.¹

Law enforcement agencies’ use of Clearview for its intended purpose likewise does not raise concerns under any other constitutional provisions that facial-recognition technology critics could invoke, such as the Fifth, Sixth, or Fourteenth Amendments. The Fifth Amendment’s Self-Incrimination Clause provides: “No person shall ... be compelled in any criminal case to be a witness against himself.” U.S. Const. amend. V. But self-incrimination jurisprudence is clear that “the Fifth Amendment is limited to prohibiting the use of ‘physical or moral compulsion’ exerted on the person asserting the privilege.” *Fisher v. United States*, 425 U.S. 391, 397 (1976) (collecting cases). It “protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature,” and “offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture”—*i.e.*, “the source of ‘real or physical evidence.’” *Schmerber v. California*, 384 U.S. 757, 761, 764 (1966). The use of Clearview by law enforcement agencies involves neither any physical or moral compulsion nor testimonial or communicative evidence.

¹ We have not analyzed whether use of Clearview raises concerns under state constitutions, some of which are more protective of “privacy” interests than the federal Constitution, including through provisions expressly recognizing a “right to privacy.” See, e.g., Alaska Const. art. I, §22 (“The right of the people to privacy is recognized and shall not be infringed.”); *City of Seattle v. Mesiani*, 755 P.2d 775, 776 (Wash. 1988) (noting that Washington Constitution “provides greater protection to individual privacy interests than the Fourth Amendment”). Nevertheless, we are not aware of any cases construing state constitutions in a manner that would present any problems for Clearview’s use by law enforcement.

KIRKLAND & ELLIS LLP

The Fifth Amendment's Due Process Clause provides that "[n]o person shall ... be deprived of life, liberty, or property, without due process of law," U.S. Const. amend. V, and the Fourteenth Amendment's Due Process Clause similarly provides, "nor shall any State deprive any person of life, liberty, or property, without due process of law," U.S. Const. amend. XIV, §1. At its core, "due process" protects against arbitrary government action. See *Wolff v. McDonnell*, 418 U.S. 539, 558 (1974) ("The touchstone of due process is protection of the individual against arbitrary action of government."). But "only the most egregious official conduct can be said to be 'arbitrary in the constitutional sense.'" *Cry. of Sacramento v. Lewis*, 523 U.S. 833, 846 (1998) (quoting *Collins v. City of Harker Heights*, 503 U.S. 115, 129 (1992)). So long as government authorities use Clearview's facial-recognition technology in the appropriate manner—namely, as an additional investigative tool but not as evidence in court to demonstrate probable cause to obtain a warrant or otherwise—there is no colorable argument that its use is arbitrary, egregious, or otherwise implicates due process concerns.

The Sixth Amendment's Confrontation Clause provides: "In all criminal prosecutions, the accused shall enjoy the right ... to be confronted with the witnesses against him." U.S. Const. amend. VI. Under Supreme Court jurisprudence, that Clause "guarantees a defendant's right to confront those 'who "bear testimony"' against him." *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 309 (2009) (quoting *Crawford v. Washington*, 541 U.S. 36, 51 (2004)). The Clause extends to "testimonial statements," such as affidavits or other "solemn declaration[s] or affirmation[s] made for the purpose of establishing or proving some fact." *Id.* at 310 (citation omitted). When used as intended, Clearview does not implicate the Confrontation Clause; neither it nor its results are intended to be used in court, and it is not designed to provide any sort of evidence to be used "for the purpose of establishing or proving some fact." As such, it falls outside the scope of Confrontation Clause jurisprudence.

Finally, the Fourteenth Amendment's Equal Protection Clauses provides: "[N]or shall any State ... deny to any person within its jurisdiction the equal protection of the laws." U.S. Const. amend. XIV, §1. Identification processes have been criticized on these grounds in the past due to, for example, the so-called "cross-race effect," which is the idea "that people are generally less accurate at identifying members of other races than they are at identifying members of their own race." *Commonwealth v. Bastaldo*, 32 N.E.3d 873, 880 (Mass. 2015). The existence of such an effect "has reached a near consensus in the relevant scientific community and has been recognized by courts and scholars alike." *Id.* at 880-81. Clearview's facial-recognition technology, however, does not involve any demographic information, and does not depend on the use of any protected class or characteristics. As discussed in more detail below, Clearview in fact promotes equal protection principles by relying wholly on objective facial-recognition technology that helps eliminate the risk of implicit bias and human error.

KIRKLAND & ELLIS LLP

B. Law Enforcement Agencies' Use of Clearview For Its Intended Purpose is Consistent with State Biometric and Privacy Laws.

While there are not yet any federal biometric or privacy laws addressing facial-recognition technology, an increasing number of states have enacted legislation that could implicate such technology. Although we have not conducted an exhaustive review of every potentially relevant law, law enforcement agencies' use of Clearview for its intended purpose does not appear to violate those laws. These laws are not aimed at government agencies that use services like Clearview or Google, and instead are directed at the capture or use of biometric data for commercial purposes. By using a service like Clearview or Google, law enforcement organizations are neither capturing biometric data nor using it for commercial purposes. In addition, some laws expressly exempt governmental entities from their reach.

For example, Washington's biometric law provides that "[a] person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose." Wash. Rev. Code. §19.375.020. Not only is this provision limited to a "commercial purpose," but the statute provides a definition of "commercial purpose" that expressly carves out law enforcement. *See id.* §19.375.010(4) ("Commercial purpose" means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier. 'Commercial purpose' does not include a security or law enforcement purpose.").

Similarly, Illinois's Biometric Information Privacy Act places limits on what a "private entity" may do with "biometric identifiers or biometric information." 740 ILCS 14/15. But a law enforcement agency is not a "private entity," for the law provides that "[a] private entity does not include a State or local government agency." 14/10. And California's forthcoming Consumer Privacy Act, which will go into effect in 2020, applies only to a "business," the conditions for demonstrating which—for example, having annual gross revenues in excess of \$25 million—would not apply to governmental organizations like law enforcement. Thus, whatever effect such state laws may have on the assembly and commercialization of databases, these laws by their terms do not restrict law enforcement agencies' ability to use tools like Clearview and Google.²

² This conclusion is reinforced by the fact that a handful of municipalities—including San Francisco and Oakland, California—have barred law enforcement from employing facial-recognition technology. Thus, when jurisdictions wish to prohibit the use of facial-recognition technology by law enforcement, they do so through direct regulation of law enforcement, and not by relying on laws addressing the collection or use of biometric information.

KIRKLAND & ELLIS LLP

II. Law Enforcement Agencies' Use of Clearview For Its Intended Purpose Promotes Constitutional Values.

Not only is law enforcement agencies' use of Clearview for its intended purpose legally permissible; based on our understanding of the product, the correct use of Clearview serves some important constitutional values better than alternative investigative techniques. By using computer searches, publicly available information, and race-neutral techniques, the use of Clearview by law enforcement avoids some of the difficulties implicated by more traditional techniques.

Clearview's technology is state-of-the-art. Clearview's engineers have developed cutting-edge facial-recognition tools that can return accurate matches of an uploaded image within seconds. Kirkland & Ellis attorneys have used the Clearview application and found that it returns fast and accurate search results. But powerful matching software is only half of the technology story. The other half is Clearview's database, which as we understand it includes billions of publicly available images. Clearview is constantly enlarging and updating this database and thus constantly enhancing the accuracy of the search results based on a user-uploaded image.

The combination of Clearview's matching software and its image database results in an effective facial-recognition tool for law enforcement agencies. The proof is in the results. Over 200 law enforcement agencies around the nation currently use Clearview. These entities frequently report that, within months, if not days, of obtaining Clearview, they have used the application to identify suspects and solve or advance cases that would otherwise likely remain open. Among other examples:

- **Child exploitation:** A child exploitation investigations unit had been investigating a major child pornography/exploitation operation. They were reviewing a series of photographs that contained the image of a male's face in the background. Agents searched the face against available criminal databases to no avail until they used Clearview. With Clearview, the subject male in the photo was instantly identified.
- **Theft:** On one agency's very first day using Clearview, it received an intelligence bulletin seeking assistance in identifying a theft suspect. The picture on the bulletin was uploaded to Clearview, which provided two possible matches. The information was sent to the requesting agency and the suspect was apprehended.
- **Narcotics:** Investigators received information regarding a narcotics dealer, but all the information they had was a social media profile with a nickname. An image was obtained from the profile and uploaded to Clearview, which provided a possible match with a real name attached, allowing investigators to positively identify the subject.
- **Bank fraud:** A group of individuals using fake identification was conducting a series of fraudulent bank transactions. The case grew cold because investigators were unable to determine the true identities of the subjects. The only real clues were several bank surveillance images of some of the subjects. These images were uploaded to Clearview,

KIRKLAND & ELLIS LLP

which brought back a Georgia arrest mug shot that revealed the true identity of one of the individuals.

- **Robbery:** A male subject robbed a retail store with a handgun. The subject was later apprehended and taken into custody, but provided several different names along with different social security numbers. Using Clearview, law enforcement determined the subject's true identity in a matter of seconds, and subsequently determined that he had outstanding warrants in three different states for violent felonies.
- **Human trafficking:** An agency received an intelligence bulletin regarding a subject possibly involved in human trafficking. The bulletin's image was uploaded to Clearview, which provided numerous possible results, as well as direct links to various social media accounts belonging to the subject. Through further investigation, a name was identified and provided to the applicable agency. Its investigators were able to watch videos from one of his social media pages, which discussed human trafficking.
- **Sexual assault:** Investigators were working a sexual assault case and needed to make contact with a mobile-app driver who transported the victim to her residence the night of the incident. All that was available was an electronic receipt with an image of the driver. The image was uploaded to Clearview, which returned three possible matches with a name attached. The subject was positively identified, and the investigator was able to contact the subject for an interview.

At the same time that Clearview has proven an effective law enforcement tool, based on our understanding of its operations, Clearview's technology minimizes the use of race in investigative law enforcement while reducing the need for some more traditional techniques with their own risks to privacy values. Some have criticized facial-recognition technology for purportedly misidentifying minorities at a higher rate than non-minorities, or otherwise increasing the potential for inherent human biases. As an initial matter, given the fast pace of technological developments in this field, many of these criticisms are dated or misleading. For example, one often-cited study from MIT was published in January 2018, and thus addresses technology from 2017 and before—a veritable lifetime in the rapidly evolving field of facial recognition. In addition, supposed "tests" on facial-recognition technologies are often not performed consistently with how the service is designed to be used by law enforcement. For instance, in July 2018, the American Civil Liberties Union reported that another company's facial-recognition technology incorrectly matched 28 members of Congress with people who had been arrested, with a disproportionate number of minority legislators misidentified. But the test had been run with a "confidence threshold" of 80 percent, while the company's recommended threshold for law enforcement work was 95 percent.

In any event, as we understand it, Clearview's cutting-edge technology avoids pitfalls from the use of racial or related factors. Other facial-recognition companies frequently use additional demographic inputs in their algorithms to narrow the results returned in an image search. This can become problematic and perpetuate human error based on perceived demographic characteristics—just as traditional identification techniques, such as eyewitnesses and police

KIRKLAND & ELLIS LLP

lineups, can suffer from human failings, including failings related to perceptions (or misperceptions) about race. By contrast, Clearview's technology uses only objective facial-recognition technology and has no demographic inputs. It simply matches faces. By using wholly objective and technological criteria, Clearview avoids returning results improperly influenced by race, ethnicity, or gender. Indeed, underscoring Clearview's superiority in this regard, Clearview recently ran the same "test" on members of Congress that the ACLU ran in 2018 using another company's technology. In fewer than *three seconds* per search, Clearview matched *every* legislator with *100%* accuracy.

At the same time that Clearview's non-race-based algorithms avoid some of the biases of more traditional identification techniques, the ability of law enforcement officials to use cutting-edge technologies to identify suspects eliminates the need for other techniques with their own costs for privacy and civil liberties. A law enforcement agency that uses Clearview to identify a suspect from a user-uploaded image, such as an ATM photograph or cell phone photograph taken by a witness, and then uses Google or comparable services to gather additional information about that individual, can avoid the need to canvass neighborhoods near the crime scene or to stop and question potential witnesses of the crime. While the privacy and civil liberty costs of those more traditional techniques are familiar and tolerable, they are not inconsequential. Thus, any consideration of the privacy or civil liberties implications of new technology cannot evaluate that new technology in a vacuum, but must consider the law enforcement activity that the new technology displaces. Empowering law enforcement officials with technology, like Clearview, that narrows the universe of suspects and provides critical information that traditionally required numerous interactions between law enforcement and the public has the potential to serve the basic values underlying the Fourth Amendment.



Clearview AI's mission is to drastically reduce crime, fraud and risk in order to make communities safer and commerce secure.

Our proprietary image database in combination with the world's best facial-recognition technology enables Clearview AI to identify individuals from a simple headshot.

In 2018, Clearview AI began solving crimes using newly developed facial-recognition technology to identify wanted criminals from newspaper stories.

On September 24, 2018, *The Gothamist* published a photo of a man who assaulted two individuals outside a bar in Brooklyn, NY. Using Clearview, the assailant was instantly identified from a large-scale, curated image database and the tip was delivered to the police, who confirmed his identity.

On December 1, 2018, *The Daily News* published a photo of a man who "fondled a woman's butt" on a NYC subway. Clearview made an instant identification and sent the tip to the NYPD. The assailant was soon apprehended. Within a matter of weeks, a small team of police detectives was able to solve 40 cold cases using Clearview.

Clearview's speed and accuracy are unsurpassed. **But the true 'secret sauce' is data – mountains of it.** No other provider offers a large-scale, curated image database combined with advanced facial-recognition technology. Data is what transforms Clearview from merely great software into a powerful tool that can solve crimes, identify fraud and dramatically reduce risk.

How Face Search Works

HOW CLEARVIEW'S TECHNOLOGY CAN HELP YOU FIND A NEEDLE IN A HAYSTACK



For More Information: Jessica@clearview.ai

Stop Searching. Start Solving.

Human Trafficking: An intelligence bulletin was received in reference to a subject possibly involved in human trafficking. The image from the bulletin was uploaded to Clearview, which provided numerous possible results. The source information provided by Clearview allowed a direct link to various social media accounts that belong to the subject. Through further investigation, a name was located and provided to the applicable Sheriff's Office. Their investigators were able to watch videos from one of his social media pages, which discussed human trafficking.

Child Exploitation: A child exploitation investigations unit had been investigating a major child pornography/ exploitation case. They were reviewing a series of photographs that contained the image of a male's face in the background. Agents searched the face against available criminal databases to no avail until they discovered Clearview AI. With Clearview AI, the subject male in the photo was identified.

Theft: The first day we gained access to Clearview, we received an intelligence bulletin from a Florida Sheriff's Office in reference to identifying a theft suspect. The picture provided on the bulletin was uploaded to Clearview, which provided two possible matches, both of which were mugshots from previous arrests in Florida. The information was sent to the Sheriff's Office and the suspect was apprehended.

Theft: A male subject committed a felony theft at a telecommunications store. The theft was caught on surveillance cameras inside the store. A still shot was obtained from the video and uploaded to Clearview. Clearview did not provide a possible match initially, but it did provide a tab to review similar results (images of subjects that have the same facial characteristics). Upon reviewing these results, an image was located that appeared similar to the suspect. Because of the source information provided by Clearview, we were able to locate and identify the suspect who currently lives in Michigan. Felony warrants have been obtained for the suspect.

Sexual Assault: Investigators were working a sexual assault case and needed to make contact with a mobile app driver that transported the victim to her residence the night of the incident. We were provided an electronic receipt with an image of the driver, but no identifying information. The image was uploaded to Clearview with three possible matches with a name attached. The subject was positively identified, and the investigator was able to contact the subject for an interview.

Narcotics: Narcotics investigators received information on a narcotics dealer in our city, but all the information they had was a social media profile with a nickname. An image was obtained from the profile and uploaded to Clearview, which provided a possible match with a name attached. Narcotics investigators were able to positively identify the subject and further their investigation.

Counterfeit Currency Case: While assisting a local Police Department, surveillance image of male passing counterfeit money at a grocery was developed and the subject image was run through Clearview AI. Even though he was hiding long dreadlocks under a baseball cap, the subject's social media page was brought back as a hit and a perusal of pictures on his social media confirmed he had worn similar ball caps before and revealed a distinctive tattoo. A local police department is in the process of issuing state warrant for passing counterfeit currency.

Bank Fraud: A group of fraudsters using synthetic IDs (i.e. the names of the subjects and all identifiers are fake) was conducting a series of fraudulent bank transactions and the case grew cold because the agents were unable to determine the true identities of the subjects. The only real clues were several bank surveillance images of 5-6 subjects. One of these images revealed a male with distinctive hair style and a search in Clearview AI brought back a Georgia arrest mug shot that revealed his true identity. The federal government is continuing its bank fraud case.

Fake Driver's License: An agent out in the field called on 6/27/19 and said a subject was using a fake Georgia Driver's License and wouldn't reveal their true identity. Clearview AI brought back a Georgia arrest mugshot of an individual with a history of fraud. The applicable Sheriff's Office is pursuing state charges for fake identification.

Time is law enforcement's most valuable resource. Clearview puts the world's most advanced facial-recognition technology and largest image database into their hands, allowing them to turn a photograph into a solid lead in an instant.



Stop Searching. Start Solving.

Bank Fraud: A private bank investigator posted a BOLO of a female impersonating a customer the first week July 2019 and then a local law enforcement detective posted other images from a different bank branch of the same subject on 7/11/19 depositing a fake check over \$30K. A Clearview AI search brought back Instagram images of this subject who is a model in the Atlanta area. In late June 2019, another female subject committing bank fraud was analyzed in Clearview AI and through certain social media evaluation her substance abuse problem was revealed. This information was delivered to appropriate fraud investigators. The police and fraud investigators now have a name and will continue their fraud investigations.

Robbery: On the night of April 18, 2019, a male subject entered a retail store with a handgun and robbed the store taking an undetermined amount of cash. The male subject was later apprehended and taken into custody. Once arriving at the station, the subject provided several different names along with different social security numbers. Using Clearview we secured the subjects identity in a matter of seconds, then ran the subjects name through NCIC and discovered that the person had outstanding warrants in another city in Alabama for two counts of Robbery; several felonies in Georgia, and escape and other charges in North Carolina.

Romance Scams: The true identity associated with over a dozen images posted by fraudsters to commit fraud on lonely individuals on dating sites have been successfully analyzed through Clearview AI. The victims have been deceived into sending thousands of dollars to international fraudsters. The victims were informed that their new on-line romance isn't the person in the picture, and they need to stop sending money to these international fraudsters.

Robbery: A 90-year-old woman was robbed and assaulted and beaten in a public parking lot in a rural town by an unknown suspect. The local police department sent into the state attorney general's office an image of an African-American female and an African-American male to be scanned by Clearview. The female image was scanned first and returned images of both a man and a female. The attorney general's office contacted the local police department and inquired as to what exactly he was supposed be looking for because the analysis provided both images of a man in a female. It turned out that the female image was actually indeed a male dressed up like a female. The technology had no bias toward gender or cosmetic adornments to identify the true suspect that posed himself as a man at times and a female at other times. The name variations were similar between the two images. The female version uses a slight reversed variation of the male's name. The suspect has fled the state and is being pursued.

Testimonials:

"The Clearview App was instrumental in this investigation. Identifying this person would have taken weeks to months using the conventional fingerprint method. There is no doubt the Clearview App is a wonderful tool to add to the duty belt of law enforcement." -Chief of Police

"Not only has Clearview allowed our agency to solve a felony theft case, contact a subject involved in a sexual assault case, and identify a narcotics dealer, but it has also allowed us to help a neighboring agency and a neighboring state. Clearview is an invaluable resource to use while gathering intelligence information for our investigators and patrol officers. It also allows us to assist other agencies who may not have access to such a useful resource. Through networking with other agencies within other states, we are able to receive LEO bulletins requesting assistance to attempt to identify suspects. As proven by the assistance we provided, we are able to get some heinous people off the streets and hopefully save some people's lives in the process." – Intelligence Officer

Time is law enforcement's most valuable resource. Clearview puts the world's most advanced facial-recognition technology and largest image database into their hands, allowing them to turn a photograph into a solid lead in an instant.



Stop Searching. Start Solving.

Clearview provides clients with its proprietary technology, database and investigative tools on a subscription basis. A Licensed User's subscription includes:

- ✓ Unlimited Use of CV's Proprietary Research System for its Licensed Users.
- ✓ Unlimited Access to CV's Proprietary Image Database for its Licensed Users.
- ✓ Each Licensed User Account Includes iPhone/Android CV Application
- ✓ Each Licensed User Account Includes Lap/Desktop Versions of CV Program
- ✓ Help-Desk Support

Annual 12-month Subscription Rates

5 Seats: \$10,000
10 Seats: \$15,000
20 Seats: \$25,000
50 Seats: \$50,000
125 Seats: \$100,000
500 Seats: \$250,000

Unlimited License (Unlimited Users): Negotiated Flat Fee

For More Information: Jessica Medeiros Garrison
(e) Jessica@clearview.ai (c) 205.568.4371

Time is law enforcement's most valuable resource. Clearview puts the world's most advanced facial-recognition technology and largest image database into their hands, allowing them to turn a photograph into a solid lead in an instant.



Tax ID: 82-2397610

Clearview Ai, Inc.
15 West 72nd St. Suite 23-S New York, NY 10023

Our office spent 12 man hours over a month's time trying to identify a theft suspect. We ran the picture through Clearview and identified the suspect in seconds.



If we had Clearview at the time when the report came in, we would not only have identified the suspect sooner, but also would have prevented other thefts that the suspect committed before we arrested him.

John Hodgens
Police Officer



World's best facial-recognition technology combined with the world's largest database of headshots.

Real-time Results.

On September 24, 2018, *The Gothamist* published a photo of a man who assaulted two individuals outside a bar in Brooklyn, NY.

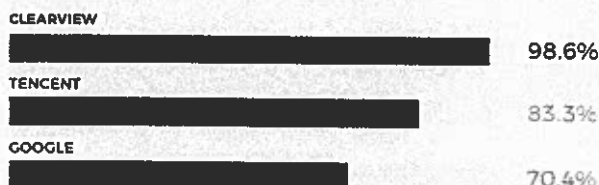
Two Men Assaulted After Leaving Williamsburg Gay Bar



World-Class Accuracy.

Clearview consistently ranks ahead of the world's leading providers in accuracy (Source: Megaface)

Accuracy finding a match out of 1 Million faces:



 **Clearview Ai**

CITY OF ATLANTA
DEPARTMENT OF PROCUREMENT
55 TRINITY AVENUE, S.W., SUITE 1900
ATLANTA, GEORGIA 30303-0307
Phone: (404) 330-6204
Fax: (404) 658-7705



PURCHASE ORDER	
Purchase Order	52004002
Purchase Order Date	24-SEP-2019
Print Date	24-SEP-2019
Revision	0
Revision Date	24-SEP-2019
Release	24-SEP-2019
Buyer	Angela Brown
Buyer Phone #	1-404-546-1713

SUBMIT INVOICE TO: BILL TO ADDRESS

APPROVED

To:
Clearview AI, Inc.
15 West 72nd Street
Suite 23-S
New York NY 10023 US

Bill To:
COA Dept Of Finance
Accounts Payable Division
68 Mitchell Street
Suite 6100
Atlanta, GA 30303

NOTE: YOU ARE RESPONSIBLE FOR ADHERING TO THE GENERAL TERMS AND CONDITIONS (REVISED 06.JUN.19) LOCATED HERE AND ATTACHED.

UNLESS SPECIFICALLY INDICATED BELOW, ALL ITEMS ON THIS ORDER ARE F.O.B. DESTINATION, UNLOADED. THE BELOW LISTED NUMBER IS THE FEDERAL EXCISE TAX EXEMPTION NUMBER, AS ASSIGNED BY THE INTERNAL REVENUE SERVICE AND NO FURTHER EXEMPTION IS NECESSARY. RIGHT IS RESERVED TO CANCEL ORDER IF DELIVERY IS NOT MADE AS AGREED.

F.O.B	Terms	Ship Via	Contract	Federal Tax Exempt #
FOB DST PPD	Net 30			586000511

Line No.	Need by Date	Item Description/Ship To Address	Qty	UOM	Unit Price	Line Total
1	2019-10-01	APD-CID/SES/CRIMINAL INTEL/DAN WORRELL. CLEARVIEW AI. -Clearview AI licenses. Ship To: 930 APD ANNEX 3493 Donald Lee Hollowell Parkway, NW Atlanta GA 30331 US Department Contact: Daniel Worrell 1-470-226-6661	6,000.00	USD	\$6,000.00	\$6,000.00

TOTAL : 6,000.00

THE UNDERSIGNED HEREBY CERTIFIES THAT HE/SHE IS AN OFFICIAL OF THE CITY OF ATLANTA, AND THIS MERCHANDISE IS PURCHASED FOR SUCH GOVERNMENTAL AGENCY AND IS TAX EXEMPT

<i>David L. Worrell</i>	24-SEP-2019
CHIEF PROCUREMENT OFFICER	DATE

City of Atlanta Standard Purchase Order Terms and Conditions

1. Correct Purchase Order and Stock Numbers must appear on all packages, invoices, shipping papers and correspondence packing slips must accompany all shipments.
2. Invoice Instructions: All invoices are to be mailed to Bill-To address. Any invoice that does not reference the City of Atlanta's Purchase Order number will be returned to the vendor unpaid.
3. Enter our order for the items or services decided subject to conditions set forth in this Order and on the reverse side hereof. Important- This Order expressly limits acceptance to terms stated herein, and any additional or different terms proposed by the Seller are rejected unless expressly agreed to in writing.
4. Unsatisfactory delivery schedule or service will be sufficient cause for cancellation of this Order at no expense to Buyer.
5. Seller and Buyer agree as follows:
 - a. Seller to Package Goods- Seller will package good in accordance with good commercial practice. Each shipping container shall be clearly and permanently marked as follows:
 - i. Seller's name and address
 - ii. Consignee's name, address, and purchase order or purchase release number and the supply agreement number if applicable
 - iii. Container number and total number of containers, e.g. box 1 of 4 boxes
 - iv. The number of containers bearing the package slip. Seller shall bear cost of packaging unless otherwise provided.
6. Terms of payment shall commence on the date of receipt by Buyer's designated purchasing office of an invoice, conforming with Buyer's purchase order. Return of the invoice by Buyer to Seller for any reason not attributable to the fault of the Buyer will extend the discount periods so that it commences on the subsequent date of receipt of such invoice by Buyer.
7. Do not substitute material on this Order without authority from Purchasing Department. All material furnished must be as specified and will be subject to inspection and approval of Buyer after delivery. Buyer reserves the right (Payment notwithstanding) to reject and return, at the risk and expense of the Seller, such portion of any shipment which may be defective or fails to comply with specifications, without invalidating the remainder of the order.
8. Unless otherwise provided herein or by law, Seller shall pay all sales, use, excise, and other taxes, charges and contributions now or hereafter imposed on, or with respect to or measured by either the goods furnished hereunder, or the compensation paid to persons employed in connection with performance hereunder, and Seller shall indemnify Buyer against any liability and expense by reason of Seller's failure to pay the same.
9. Seller warrants

City of Atlanta Standard Purchase Order Terms and Conditions

- a. That each and all of the articles herein described are free from defects in design, workmanship, and materials
 - b. That unless otherwise specified herein all such articles and the components thereof are new and have not been previously used
 - c. That the said articles are fit for use for their ordinary intended purposes and any purposes specified herein
 - d. That each and all of the articles herein described and the sale and use thereof will not constitute infringement or contributory infringement of any patent, or infringement of any copyright or trademark, or violation of any trade secret
 - e. That none of the chemical substances sold or transferred under this Purchase Order to buyer as of the time of such sale or transfer, is on the list of chemical substances compiled and published by the administrator of the EPA pursuant to the Toxic Substances Control Act (Title 15 U.S.C. §2601 et seq.)
10. Seller shall indemnify and hold Buyer and its employees harmless from and against any and all claims, suits, judgement or expenses (including attorney's fees) which are grounded or based wholly or partially upon alleged negligence or actual negligence in the formation or manufacture of any merchandise sold by the Seller to the Buyer hereunder, or upon any alleged defect or actual defect in the merchandise, or upon a claim that the merchandise was not of merchantable quality or that it was not fit for the purposes for which it was intended.
11. Either Seller or Buyer shall be excused from performance of the obligations hereunder when and to the extent that such performance is delayed or prevented by any circumstances reasonably beyond control, or by fire, explosions, any strike or labor dispute, or any act of omission of any governmental authority.
12. The vendor or contractor warrants that it has not employed or retained any company or person, other than a bona fide employee working for the vendor or contractor, to solicit or secure this contract or purchase order, and that the vendor or contractor as not paid or agreed to pay any person, company, association, corporation, individual or firm, other than a bona fide employee working for the vendor or contractor, any fee, commission, percentage, gift or any other consideration contingent upon or resulting from the award or making of this provision. For the breach or violation of the above warranty and upon finding after notice and hearing, the City shall have the right to terminate the purchase order or contract without liability, and at its discretion, to deduct from the contract or purchase order price, or otherwise recover the full amount of such fee, commission, percentage, gift, or consideration.
13. This contract can be modified or rescinded only by a writing signed by both of the parties or their duly authorized agents.
14. No claim or right arising out of a breach of this contract can be discharged in whole or in part by a waiver or renunciation of the claim or right unless the waiver or renunciation is supported by consideration and is in writing signed by the aggrieved party.

City of Atlanta Standard Purchase Order Terms and Conditions

15. Prohibition Against Assignment: It is the intent of the parties that the terms printed herein will control irrespective of any subsequent execution for a work order, receipt, purchase order, or similar instrument. This agreement shall be binding on the parties hereto their successors and assigns. Seller shall not assign this agreement. Any attempt to assign this agreement shall cause this agreement to be terminated by the City. The City reserves the right to refuse or reject any and all request for assignment and, may in its discretion, terminate said agreement at its convenience.

16. This agreement shall be governed by the Uniform Commercial Code. Wherever the term "Uniform Commercial Code" as adopted in the State of Georgia as effective and in force on the date of this agreement.

17. Statement of Non-Discrimination Policy:

Pursuant to Part II, Chapter 2, Division 10, Section 2-1387 of the Code of Ordinances, the City of Atlanta has implemented a policy regarding nondiscrimination by firms doing business with the City of Atlanta. Therefore, the Equal Employment Opportunity Clause, as specified in Sections 2-1414 through 2-1419 of the Code of Ordinances and Mayor's Administrative order Number 96-4, prohibiting discrimination by contractors, employees, officers, and vendors against persons on the basis of their sexual orientation, are hereby made a part of the terms and conditions of this contract.

18. The supplier of goods material, equipment, or services covered by this purchase order certifies that they will not discriminate in any way in connection with this contract in the employment of persons, or refuse to continue the employment of any such person on account of race, creed, color, sex, sexual orientation or national origin of such person.

19. Sec. 2-1414. - Equal employment opportunity clause.

The equal employment opportunity (EEO) clause required in all city contracts, pursuant to section 2-1200, shall read as follows:

"During the performance of this agreement, said contractor agrees as follows:

(a) The contractor shall not discriminate against any employee, or applicant for employment, because of race, color, creed, religion, sex, domestic relationship status, parental status, familial status, sexual orientation, national origin, gender identity, age, disability, or political affiliation. As used here, the words "shall not discriminate" shall mean and include without limitation the following:

Recruited, whether by advertising or other means; compensated, whether in the form of rates of pay, or other forms of compensation; selected for training, including apprenticeship; promoted; upgraded; demoted; downgraded; transferred; laid off; and terminated.

The contractor agrees to and shall post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officers setting forth the provisions of the EEO clause.

(b) The contractor shall, in all solicitations or advertisements for employees,

City of Atlanta Standard Purchase Order Terms and Conditions

placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, creed, religion, sex, domestic relationship status, parental status, familial status, sexual orientation, national origin, gender identity, age, disability, or political affiliation.

(c) The contractor shall send to each labor union or representative of workers with which the contractor may have a collective bargaining agreement or other contract or understanding a notice advising the labor union or workers' representative of the contractor's commitments under the equal employment opportunity program of the City of Atlanta and under the Code of Ordinances and shall post copies of the notice in conspicuous places available to employees and applicants for employment. The contractor shall register all workers in the skilled trades who are below the journeyman level with the U.S. Bureau of Apprenticeship and Training.

(d) The contractor shall furnish all information and reports required by the contract compliance officer pursuant to the Code of Ordinances, and shall permit access to the books, records, and accounts of the contractor during normal business hours by the contract compliance officer for the purpose of investigation so as to ascertain compliance with the program.

(e) The contractor shall take such action with respect to any subcontractor as the city may direct as a means of enforcing the provisions of paragraphs (a) through (h) herein, including penalties and sanctions for noncompliance; provided, however, that in the event the contractor becomes involved in or is threatened with litigation as a result of such direction by the city, the city will enter into such litigation as is necessary to protect the interest of the city and to effectuate the equal employment opportunity program of the city; and, in the case of contracts receiving federal assistance, the contractor or the city may request the United States to enter into such litigation to protect the interests of the United States.

(f) The contractor and its subcontractors, if any, shall file compliance reports at reasonable times and intervals with the city in the form and to the extent prescribed by the contract compliance officer. Compliance reports filed at such times directed shall contain information as to employment practices, policies, programs and statistics of the contractor and its subcontractors.

(g) The contractor shall include the provisions of paragraphs (a) through (h) of this equal employment opportunity clause in every subcontract or purchase order so that such provisions will be binding upon each subcontractor or vendor.

(h) A finding, as hereinafter provided, that a refusal by the contractor or subcontractor to comply with any portion of this program, as herein provided and described, may subject the offending party to any or all of the following penalties:

(1) Withholding from the contractor in violation all future payments under the involved contract until it is determined that the contractor or subcontractor is in compliance with the provisions of the contract;

(2) Refusal of all future bids for any contract with the City of Atlanta or any

City of Atlanta Standard Purchase Order Terms and Conditions

of its departments or divisions until such time as the contractor or subcontractor demonstrates that there has been established and there shall be carried out all of the provisions of the program as provided in the Code of Ordinances;

(3) Cancellation of the public contract;

(4) In a case in which there is substantial or material violation of the compliance procedure herein set forth or as may be provided for by the contract, appropriate proceedings may be brought to enforce those provisions, including the enjoining, within applicable law, of contractors, subcontractors or other organizations, individuals or groups who prevent or seek to prevent directly or indirectly compliance with the policy as herein provided.

Control # _____
(Obtain Control # through Procurement Control Number Generator)

Page 1 of

Page 1 of

Requesting Division		Section	Unit
CID	SES	Criminal Intel	
Contact Person/PRO		Email	
Dan Worrell		dworrell@atlantaga.gov	
Phone	Fax	Date	
4045467916	n/a	9/4/2019	
FORMAL QUOTES ATTACHED		Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>

Company Preferred		Contact Person	
Clearview AI		Jessica Garrison	
Address			
145 W. 41 st St.			
City/State/Zip		Phone	
New York City, NY 10036		205)568-4371	
Email	Fax	SS# or FED Tax ID	
jessica@clearview.ai	n/a	n/a	

Item	Detail Description (Must include make/size/color/etc)	Qty	Contract Item#/ Catalog#/Page# (attach copy if applicable)	Model/ Part/ Product #s	Price Per Unit	Total Price
1	Clearview AI	3	n/a	Clearview Licenses	\$2,000	\$6,000
Justification of request: Clearview will assist the department with identifying suspects through facial recognition.					SUBTOTAL (of attached pages)	\$6,000
					GRAND TOTAL	\$6,000

Justification of request: Clearview will assist the department with identifying suspects through facial recognition.

For FMU Use Only

Date 6-7-19

Date 9-7-2019

Date 9/12/2019

Date _____

Date _____

Date Received	
Date Processed	
Entered By	
FAC #	
P.O. #	



CLEARVIEW AI PRICING

Clearview provides clients with its proprietary technology database and investigative tools on a subscription basis

EACH SUBSCRIPTION/SEAT INCLUDES:

- Unlimited Use of CV's Proprietary Research Technology
- Unlimited Access to CV's Proprietary Image Database
- Each User Account Includes iPhone & Desktop Versions of CV
- Help-Desk Support

Annual 12-month Subscription Rates

5 Seats:	\$10,000
10 Seats:	\$15,000
20 Seats:	\$25,000
50 Seats:	\$50,000
125 Seats:	\$100,000
500 Seats:	\$250,000

Sinks, Ryan E.

Subject: FW: Clearview facial rec
Attachments: Clearview AI - Pricing - 2019.pdf

From: Worrell, Daniel <dworrell@AtlantaGa.Gov>
Sent: Thursday, July 25, 2019 6:24 PM
To: Sinks, Ryan E. <resinks@AtlantaGa.Gov>; Vayens, Benjamin J <BVayens@AtlantaGa.Gov>
Subject: Clearview facial rec

Spoke to a representative today about the software. It is \$2,000 a year per license,

Investigator Dan Worrell
Criminal Intelligence Unit
Atlanta Police Department
226 Peachtree St SW
Atlanta, GA 30303
Office: 404-546-7916
Cell: 470-426-2364
dworrell@atlantaga.gov
daniel.worrell@leo.gov



575 Anton Blvd., Costa Mesa, CA 92626

Veritone Quote Number: 0052137

Date of Quote: 8/22/19

Quote Valid Through: 9/31/19

LICENSEE & SERVICE INFORMATION

Agency Name: Atlanta Police Department

Contact Name: John Quigley

Agency Address: 226 Peachtree St. SW, Atlanta, GA. 30303

Contact Email: JQuigley@atlantaga.gov

Term: 12 months Start Date: 10/1/19

End Date: 9/30/20

QTY	Product	Description	Line Total
1	Veritone iDentify Application	Veritone aiWARE™ Platform Access + iDentify Application	\$ 42,000
5	iDentify Platform Users	Platform Users to iDentify Application	Included
1	Training and Support	Standard webinar training and onboarding; phone, email and chat support	Included
		During the Term, Veritone will provide Licensee with access to the iDentify Application and the	
1	Cognitive Processing	cognitive processing specified above for content uploaded to the Platform by Licensee through the iDentify Application	Included
		Total	\$ 42,000

Master License Terms and Conditions: This Agreement and Licensee's access to and use of the Platform and Services are governed by the Veritone Master License Terms and Conditions at <https://www.veritone.com/terms-conditions> (the "Terms and Conditions"). In the event of any conflict or inconsistency between the provisions of this Agreement and the provisions contained in the Terms and Conditions, the provisions of this Agreement shall govern and control. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Terms and Conditions.

8 Pricing

NEC is pleased to offer APD the proposed NeoFace WideNet service for an annual fee. The following table summarizes the components and services provided during the contract term.

Table 4: NeoFace WideNet Services Pricing

NEOFACE WIDENET SERVICES PRICING	
Solution Components	
(5) concurrent NeoFace Reveal licenses	
(1) Integrated System Monitoring license	
Directory Load Tool	
Integration APIs	
Professional Services	
Implementation and Training (one-day onsite, including assistance with initial gallery load)	
Documentation	
Remote 8 x 5 Maintenance and Support	
NeoFace WideNet Annual Subscription Fee	\$75,000 per annum
Minimum contract period of five (5) years	

8.1 Conditions

- This proposal is valid for a period of 90 calendar days.
- The pricing indicates an annual fee for a minimum contract period of five (5) years.
- APD can upload up to 750,000 images and conduct up to 350 searches per day.
- 8 x 5 remote maintenance and support will be provided throughout the life of the contract.
- NeoFace WideNet is provided as a service, and as such, no warranty is provided. Additionally, NEC retains ownership of any hardware and backend software components that were provided, and they shall be returned to NEC at the end of the contract term.
- The price does not include applicable State/Federal taxes. Any taxes shall be in addition to the prices listed and if required to be collected or paid by NEC shall be paid by APD to NEC. Unless specified otherwise in this Quote, APD acknowledges that this purchase constitutes a bundled transaction or mixed transaction for sales tax purposes and, as such, is fully subject to sales tax. If claiming a sales tax or similar exemption, APD must provide NEC with valid tax exemption certificates where deliveries are to be made prior to delivery.

- Price does not include network and remote connection fees to the Microsoft Azure Government cloud.
- APD will be responsible for providing a server/workstation or a VM instance with external network connectivity and network access provided to NEC.

9 Additional Terms and Assumptions

This proposal and quote is valid for 90 days from the date of submission and should not be construed as a contractual obligation, but merely an indication to supply the goods and services indicated herein. It includes only those goods and services it specifically references, subject to the following terms and conditions.

Additional engineering effort beyond the scope of the standard solution will be quoted at a firm fixed price based on our current service rates in effect at the time of the change, plus any related travel or administrative expenses.

NEC reserves the right to substitute hardware of equal value with equal or better capability, based upon market availability. If, however, such equipment is unavailable, NEC will make its best effort to provide a suitable replacement.

Purchase orders should be sent to NEC by facsimile or United States mail. Please direct all order correspondence, including Purchase Order, to:

Raffie Beroukhim
NEC Corporation of America
10850 Gold Center Drive, Suite 200
Rancho Cordova, CA 95670
Tel: (800) 777-2347, (916) 463-7000
Fax: (916) 463-7041
Email: raffie.beroukhim@necam.com

NEC appreciates the opportunity to present this proposal. Purchase will be governed by NEC's Software as a Service Master Subscription Agreement, a copy of which is attached for your convenience in "Exhibit A – Standard Agreements."

NEC respectfully requests the opportunity to further negotiate final terms relating to these agreements. Firm delivery schedules will be provided and development will commence after APD and NEC have signed the finalized Scope of Work.

Prices are exclusive of any and all state or local taxes, or other fees or levies. No subsequent Purchase Order can override such terms. Nothing additional shall be binding upon NEC unless a subsequent agreement is signed by both parties.