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.

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

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

"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.

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.'" *Cty. 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.

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.

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,

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

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.