Sources:

* NY Times, “The Secretive Company That Might End Privacy as We Know It” - <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>
* ABC7News, “AG Bonta called to investigate Clearview AI for allegedly selling images to police without consent” - <https://abc7news.com/clearview-ai-california-attorney-general-rob-bonta-consumer-watchdog/14231840/>
* SiliconANGLE, “Despite backlash, US police are still using Clearview AI face recognition software” - <https://siliconangle.com/2023/03/28/despite-backlash-us-cops-still-using-clearview-ai-face-recognition-software/>
* The Register, “Clearview CEO doubles down, claims biz has now scraped over ten billion social media selfies for surveillance” - <https://www.theregister.com/2021/10/09/in_brief_ai/>
* The Record, “Clearview AI wins appeal to overturn $10 million UK privacy fine” - <https://therecord.media/clearview-ai-wins-uk-appeal>
* BBC News, as posted on Clearview.ai, “US police forces using facial recognition technology” - <https://www.clearview.ai/as-seen-on-tv/us-police-forces-using-facial-recognition-technology>
* NBC4 New York, “Face Recognition Tech Gets Girl Scout Mom Booted From Rockettes Show – Dut to Where She Works” - <https://www.nbcnewyork.com/investigations/face-recognition-tech-gets-girl-scout-mom-booted-from-rockettes-show-due-to-her-employer/4004677/>

**Clearview AI and The Impact of Facial Recognition on Privacy**

There are many events showcasing unethical behavior among tech giants in recent years, but arguably there is something greater than a single event which even those same tech giants view as taboo, and that is a technology: facial recognition.

In 2011, Google’s chairman at the time Eric Schmidt said, “We built that technology, and we withheld it.” In 2020 and 2021, Microsoft, Amazon, and Facebook all made announcements they would either shut down, or disallow law enforcement use of, their facial recognition technologies.

However, Manhattan-based Clearview AI takes a different stance. In Clearview’s case, both the technology and the company’s decisions and methodology in developing it are about as unethical as it gets.

Its facial recognition product is not only powerful, but continues to be utilized by law enforcement agencies across the US, despite being banned for use by law enforcement in Canada by the country’s privacy watchdog, the Office of the Privacy Commissioner (OPC), as well as being fined for around $10 million by the UK’s Information Commissioner’s Office (ICO) for unlawfully storing the images and information of UK citizens (though this fine was overturned in 2023). Clearview even posts on its own website a BBC News report stating, “The company has repeatedly been fined millions of dollars in Europe and Australia for breaches of privacy.” Clearview seems to wear its controversies as a badge of honor.

As reported by the New York Times in 2020, over 600 law enforcement agencies had begun using Clearview just within the previous year. The NYT also found the code for the app “includes programming language to pair it with augmented-reality glasses.”

The technology itself is considered unethical among most tech leaders due in part to its ability to identify individuals with nothing but a picture, giving the user access to a wealth of personal data and online activity. However, the methods used to develop the technology in Clearview’s case were also unethical. Clearview scrubbed the social media accounts of many platforms against those platforms’ terms of service, and as of 2023, had acquired over 30 billion images from personal social media pages without users’ permission.

Law enforcement can use this technology to bypass limitations of the past. Consider the following hypothetical, for example, where an individual who has never broken the law and has no record in law enforcement systems (meaning they’d have no identifying facial data in law enforcement databases) chose to take part in a protest against an instance of publicly perceived police brutality. This individual’s face was caught on the CCTV recordings of a local business where the protest took place, which was obtained by local law enforcement. A still-capture from the footage gets run through Clearview AI’s software, instantly identifying the individual. This person can now be targeted by law enforcement for any number of fabricated crimes in retaliation for their participation in the protest, even if said protest was lawful.

A hypothetical isn’t even necessary to demonstrate how this technology can negatively impact the average person. For a real-world example, consider what happened to Kelly Conlon at a Christmas show at the Radio City Music Hall. While the report from NBC New York does not state that the venue used Clearview’s software, Kelly, who attended the show with her daughter and her Girl Scout troupe, was immediately identified through facial recognition software as an attorney associated with a New Jersey based law firm who had “been involved in personal injury litigation against a restaurant venue now under the umbrella of MSG Entertainment” (Madison Square Garden Entertainment). Once identified, Kelly was barred entry and banned from the property, regardless of having no direct involvement herself with any case against MSG.

Facial recognition technology is dangerous, invasive, and based on Clearview’s methods of obtaining the data required to develop their version of the tech, inherently unethical. The technology facilitates the ability to track a person’s complete whereabouts and activities without the individual needing to have a device or tracking tag on them, using nothing but their face. There is no viable way to opt-out of this technology, especially when considering that the data collected for it was done so against multiple platforms’ TOS.