Facial Recognition Tech Enforced by Vermont AG Under State Privacy & Data Broker Laws

Aaron J. Burstein, Alyssa Z. Hutnik

March 16, 2020

Vermont Attorney General Thomas Donovan Jr. has ratcheted up ongoing scrutiny of facial recognition technology. On March 10, the Vermont AG sued facial recognition technology provider Clearview AI and moved for a preliminary injunction against the company. Clearview drew wide attention in January following the publication of a *New York Times* story that detailed how the company reportedly collected approximately three billion digital photographs, primarily by scraping them from social networks and websites. The *Times* also reported that Clearview's customers include more than 600 law enforcement agencies, which apparently may use the service to connect facial images with individuals' names.

Citing the *Times*'s story and several other public sources, the Vermont AG's complaint accuses Clearview of a wide variety of unfair and deceptive practices under Vermont's Consumer Protection Act. The AG also alleges that Clearview violated Vermont's data broker law, which went into effect in 2019, by obtaining "brokered personal information" through the "fraudulent means" of unauthorized screen-scraping. The AG is seeking broad relief against Clearview, including an injunction ordering Clearview to delete photos of Vermont residents from its database and to refrain from collecting their images going forward, restitution, disgorgement, and civil penalties of $10,000 for each image collected in violation of the Consumer Protection Act.

This post takes a closer look at the complaint's view of the privacy harms that Clearview allegedly caused and how these harms inform the Vermont AG's legal claims against the company. A key takeaway is that businesses would be well served by performing privacy due diligence and a risk assessment when exploring the use of data-driven services – from data acquisition and modeling, to marketing claims.

A Dark View of Facial Recognition's Surveillance Applications

Aside from challenging Clearview's business and data practices, the Vermont AG's complaint raises

more general concerns about facial recognition technology and describes the harms caused by Clearview's alleged conduct in sweeping terms.

Two aspects of the complaint's focus on surveillance-related harms are particularly noteworthy.

1. **Critical Take on Law Enforcement's Use.** The complaint is openly critical of law enforcement agencies' use of Clearview's database – a position that law enforcement agencies rarely take against their counterparts. But the Vermont AG's message is unmistakable: "Law enforcement's use of a massive facial recognition database, like the one described [in the complaint], essentially puts every individual in that database, whether they had ever done anything wrong or not, into a permanent, inescapable virtual line-up or 'rogue's gallery' accessible for any reason at any time.'" (Complaint paragraph 20)

2. **Naming Customers.** The complaint calls out several major companies for using Clearview's service. Although the complaint does not suggest that any of these companies acted improperly, the AG's attention is a reminder that merely using a controversial technology can create negative publicity.

The complaint goes on to portray Clearview as rushing headlong into an area that policymakers and other companies have treated with great caution. Asserting that "[o]nce entered into a facial recognition database, the individual loses an enormous amount of anonymity, privacy, and freedom," the complaint states that "businesses and policymakers have been particularly cautious regarding the implementation of facial recognition technology because the potential for misuse and the consequences of such misuse are so dire." The PI motion states that Clearview developed a "dystopian surveillance database."

The complaint also asserts, "leading-edge companies with large caches of photographic data such as Facebook and Google have declined to make a facial recognition tool available, though they have the capability to do so." According to the complaint, platforms' forbearance from developing such tools contributed to "strong social norms against the type of mass-collection and facial recognition implemented by Clearview"; and Clearview violated the reasonable expectations of consumers that were based on this norm.

Alleged Privacy Violations Under Vermont's UDAP Law

The complaint alleges that the following practices are "immoral, unethical, and unscrupulous":

- Collecting facial images by screen-scraping on third-party sites, without consent of the image owners and in violation of the sites terms of service.
- Collecting minors' images without parental consent.
- Invading consumers' privacy.
- Exposing "sensitive personal data to theft by foreign actors and criminals."
- Violating consumers' civil rights and chilling First Amendment interests in assembly and political expression.

In a separate deception count, the Vermont AG focuses on several of Clearview's claims about its privacy and data security protections, including alleged misrepresentations about consumers' ability to opt out of the database and that Clearview's processing "does not unduly affect" consumers' "interests or fundamental rights and freedoms." This count also alleges that Clearview

misrepresented the accuracy of its facial recognition matching capabilities as well as the company's success in assisting law enforcement investigations.

Alleged Violation of Vermont's Data Broker Law

Finally, the Vermont AG charges Clearview with violating Vermont's data broker law. One prohibition under the law is against acquiring "brokered personal information through fraudulent means." (For an overview of Vermont's law, including its registration requirements, see this post.) Facial images posted on social networks and other sites are, according to the complaint, "brokered personal information" because they meet the requirement of being "categorized or organized for dissemination to third parties." Clearview's use of screen scraping to acquire these images constitutes the allegedly "fraudulent means" of acquiring brokered information. The complaint, however, does not allege that the platforms that host these images are themselves data brokers.