Clearview AI chief says company's business model gaining acceptance because of US law enforcement benefits

18 Oct 2021 | 21:26 GMT | **Insight**
By Mike Swift

The founder of Clearview AI said even as its database of faces has expanded to 10 billion images, its success in helping US law enforcement catch insurrectionists and pedophiles is dampening privacy concerns despite litigation and regulatory challenges.

The founder of Clearview AI today said even as the company's database of faces has expanded to 10 billion images, its success in helping US law enforcement catch insurrectionists and pedophiles is dampening privacy concerns despite litigation and regulatory challenges.

In a rare public appearance to discuss his company, Hoan Ton-That, co-founder and CEO of Clearview, said at a conference* at Stanford University that the company is limiting its services to law enforcement agencies in the US, and that it has solved problems in disproportionate misidentification of facial templates of people who are members of racial and other demographic minorities.

Clearview's growing database of faces, obtained in many cases by "scraping" images posted publicly to social media platforms as well as from public records, proved to be "a very effective tool" for the Federal Bureau of Investigation and other law enforcement agencies in identifying and prosecuting people who participated in the attack on the US Capitol on Jan. 6.

The Department of Homeland Security used Clearview AI data in 2019 to identify a child pornographer they had been otherwise unable to find, and he said both DHS and the FBI "swear by the tool."

"We've been able to show people the positive use cases," Ton-That said. "I feel that people are coming around now that [facial-recognition use] is here to stay."

Clearview AI hasn't only dramatically enlarged its facial database but has grown from about 10 employees in early 2020 to its current 45 workers, Ton-That said. The Clearview founder said he was aware of a legal battle between hiQ and LinkedIn (see here) over data scraping when Clearview was created, but didn't expect the privacy controversy. He said the company now strictly limits its products to law enforcement.

As long he is CEO, "we will never have a consumer facial recognition app that anyone can download and use," Ton-That said.

Clearview is facing an array of privacy challenges in both federal and state courts, including litigation by the Vermont attorney general who alleges the company violated the law by scraping images posted to platforms such as Facebook and YouTube and using them for a different purpose than people who posted those images expected. Vermont Attorney General T.J. Donovan called Clearview's business model "unscrupulous, unethical, and contrary to public policy" when he sued the company in March 2020 (see here).

Clearview is also facing lawsuits in federal and state courts in Illinois, including a suit brought by the American Civil Liberties Union that says the company's business model violates the Illinois Biometric Information Privacy Act (see here). He declined to answer questions from MLex on the sidelines of the conference about those cases, saying he is not granting media interviews.

Ton-That, dressed in a pink suit, white belt and white shoes as part of an outfit that stood out at the otherwise button-down meeting of the conservative and libertarian Federalist Society, said it's an incorrect analogy to compare facial recognition with questions about more private online actions such as a Google search.

People do not expect their faces to be private. As humans, "we're born to recognize faces. So I put it in a different category" of privacy, he said.

Clearview's own testing shows the company's technology has overcome issues of artificial intelligence algorithms making

a higher rate of mistakes in identifying minority populations. "This works very well through all demographics. It's much better than the human eye," Ton-That said, saying the company's internal testing shows "zero" bias by race.

Ton-That said it's important to draw a distinction between real-time facial recognition and after-the-fact use by law enforcement agencies that are bound by due process. Most people, he predicted, will favor "giving up a little bit of privacy for a lot of security" in its use by law enforcement.

"It's kind of a hard thing to be against the technology in this kind of use case," he said.

"A National Symposium on Law & Technology in the Age of Big Tech and the Digital Leviathon," Federalist Society, Stanford University, Oct. 18, 2021.

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Related Portfolio(s):

[Data Privacy & Security - Clearview AI - Office of the Privacy Commissioner of Canada - Regulatory action over facial-recognition services (Canada)](#)
[Data Privacy & Security - Clearview AI - Joint investigation into use of 'scraped' data (Australia & UK)](#)
[Privacy - Clearview AI - ACLU's state case for alleged BIPA violations (US)](#)
[Privacy & Data Security - Clearview AI - Vermont litigation over facial data collection (US)](#)
[Data Privacy & Security - Clearview AI - Consumer IBIPA litigation over facial data recognition (US)](#)

Areas of Interest: Data Privacy & Security, Sector Regulation

Industries: Information Technology, Communication Services, Media & Entertainment, Software and Services, Media, Interactive Media & Services

Geographies: North America, United Kingdom, Australia, Vermont, Europe, USA, Canada, Oceania, European Countries

Topics:

Data Privacy   Facial recognition