Former Scam Artist Hits Jackpot

Clearview AI Phishes in Murky Waters, Catching Multiple Fines

Smile. You're on camera.

Slowly, almost imperceptibly, the surveillance state is encroaching on privacy and personal freedom, not just in China and the United States where law enforcement enjoy sweeping powers, but also in Europe. The advent of artificial intelligence has accelerated the trend, marketed as an enhancement of public security.

Curiously, the voices that advocate for small government are the same ones pushing for the state to continuously monitor its citizens, lest a few go astray. Then again, this is what modern conservatism is all about; from controlling women's bodies, to locking up entire cohorts of socially disadvantaged people, to cleansing libraries of books deemed 'inappropriate', to tracking those not yet caught in its expanding web of laws and regulations.

On Tuesday, the Dutch Data Protection Authority issued a €30.5 million fine to Clearview AI, a US corporation that scrapes the internet to gather photos and data of people. The company is not just interested in miscreants but casts a wide net and essentially wants to include everybody, preferably all earthlings.

50 Billion and Counting

Clearview AI, not to be confused with the ClearView Media Group that exploits billboards, possesses a library of over fifty billion facial images and their corresponding personal details. Your face is now owned and being monetised by Clearview AI.

The company uses this vast dataset to train its facial recognition system which can now be deployed to almost instantly identify any person filmed on any of the approximately 85 million surveillance cameras dotting US public spaces, supplemented by another 120 million or so spying eyes installed on private premises.

To identify any 'person of interest', the Clearview system only needs a partial shot of the face. The still image need not even be in sharp focus or properly illuminated. Thanks to facial recognition techniques that precisely measure the distances, angles, and topography of facial features, the biometric code this assembled delivers an individual faceprint that is almost as unique as a person's DNA.

Clearview's corporate mission of course only includes the best and noblest of intentions: it simply aims to make the world a safer place. However, the Dutch Data Protection Agency maintains that the database Clearview built is illegal. Aleid Wolfsen, the agency's chairperson, called facial recognition a "highly intrusive technology" and warned anyone in The Netherlands against doing business with the American company: "Dutch organisations that use Clearview may expect heavy fines for doing so."

Deadbeat Offender

The inclusion of Dutch nationals in the Clearview AI database is a violation of both Dutch and European privacy law. In 2021, French privacy and data collection watchdog CNIL initiated an investigation into Clearview AI's operations and practices and found the company to be in violation of the European Union's General Data Protection Regulations (GDRP), the key element, if not cornerstone, of EU privacy and human rights law.

CNIL declared Clearview AI in breach of numerous GDRP articles and accused the company of unlawfully processing personal data and of failing to take into account the rights of the individual, particularly requests for access to data. It ordered Clearview AI to cease the collection and use of 'persons on French territory' and facilitate the exercise of the individual right to demand the erasure of data.

Clearview AI did not respond to the injunction and was issued a €20 million fine plus an additional €100,000 per day of delay in implementing the CNIL demands. It has since been issued another fine of €5 million.

Whilst Clearview AI refuses to comment on its practices, the company's PR agency peddled the same old and discredited excuse that it does not have a place of business, nor customers, in the EU and thus is not subject to the GDRP. Quite maliciously, the company ignores the fact, tested and established by the courts, that the data protection regulation applies to the personal data of EU citizens which Clearview AI scraped illegally from the internet and uses and monetises without consent.

Charges A-Coming

Aleid Wolfsen, the Dutch data protection chief, admitted that it is unlikely Clearview AI will cough up the cash. However, should the company insist on ignoring European regulators, he thinks criminal charges may be brought against its founder and CEO Hoan Ton-That, resulting in a EU-wide arrest warrant.

Besides France and The Netherlands, the privacy watchdogs of Italy and Greece also imposed sizeable financial penalties on Clearview AI for flouting the law. Mr Wolfsen thinks that the agencies must now cooperate to bring the controversial US company to heel and is working towards that end.

Mr Ton-That, an Australian citizen of (royal) Vietnamese descend, is a genius of a rather singularly creepy/freakish appearance and history.

Failing to get traction with early social media apps of his design, Mr Ton-That instead turned his attention to cobbling together phishing applications and computer worms to surreptitiously obtain user data. Attempts by Australia and the UK to rein in Mr Ton-That have been shelved due to limited enforcement capacity. Basically, the Clearview CEO is hard to catch and may continue to monetise his unlawful business. Given that Mr Ton-That has a long career in hacking and phishing, it is nothing short of amazing that he has managed to evade arrest.

Hacker Goes Phishing

In 2009, Mr Ton-That - a self-described 'Anarcho-Transexual Afro-Chicano American Feminist Studies Major' - was denounced in the IT community for operating several websites that promised saucy videos to anyone logging in using their Gmail credentials. Unsuspecting users following the instructions had their computers infected by a worm of Mr Ton-That's making. This malicious code subsequently blasted a tsunami of unsolicited messages to anyone in the duped user's contact list. Google, Microsoft, and Facebook blacklisted all websites maintained and operated by Mr Ton-That.

The serial entrepreneur's luck continued after he met New York politician and former city park commissioner Richard Schwartz at the Manhattan Institute for Policy Research, an über-conservative think tank that agitates against equal rights, taxation, lenient judges, and prison reform. In 2016, the two partnered to develop an application to scrape the internet for images and their associated data - and to use their haul as the foundation of a facial recognition algorithm.

A year later, Clearview AI was launched in stealth mode to avoid revealing details of its business plan and alerting the competition. Stealth also came in handy to hide the material support of far-

right political activists, conspiracy theorists, and white supremacists. The cabal included billionaire Peter Thiel, co-founder of the intelligence gathering and mapping company Palantir, itself repeatedly embroiled in lawsuits over breaches of privacy legislation.

Mr Ton-That's credentials as a pseudo anarchists and sympathiser of far-right causes took a hit after Clearview AI started working with the US Department of Justice to identify the perpetrator of the January 6, 2021, assault on the US Capitol by supporters of Donald Trump.

BuzzFeed News, an online media company, revealed that Clearview AI provides its services to thousands of government entities and private businesses not only in North America but around the world. Within those organisations, individuals usually enjoy unrestricted and unsupervised access to Clearview's database.

Bogus

Mr Ton-That declared on Fox News that his company only worked with law enforcement agencies with 'a focus' on the United States and Canada. However, internal documents leaked to BuzzFeed show that Clearview has found many customers in retail chains, financial institutions, schools and colleges, the gaming industry, and the legal profession.

The company is also aggressively and successfully pursuing clients in Europe, South America, Asia, and the Middle East. The papers show that Clearview has more than 2,900 paying customers in addition to people (including hackers), businesses, and agencies who use the tool for free during the thirty-day trial period.

The leaked logs and record show that the company has managed to procure the business of law enforcement agencies in nearly all EU member states, including those that issued hefty fines such as France and The Netherlands.

Mr Ton-That's repeated assurances that his company refuses to engage with countries where human rights are trampled have also been exposed as bogus. Clearview has dealings with both Saudi Arabia and the UAE, and according to documents now has plans to expand into Africa.