

Facial Recognition in the Wild: All Eyes on Clearview AI

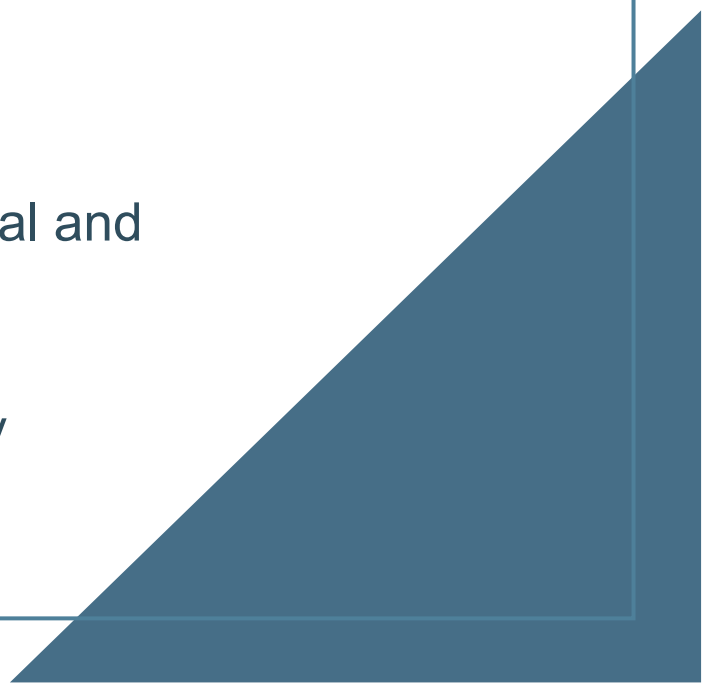
Catherine Jasserand

KU Leuven CiTIP - imec

CIF

25 November 2021

CiTIP

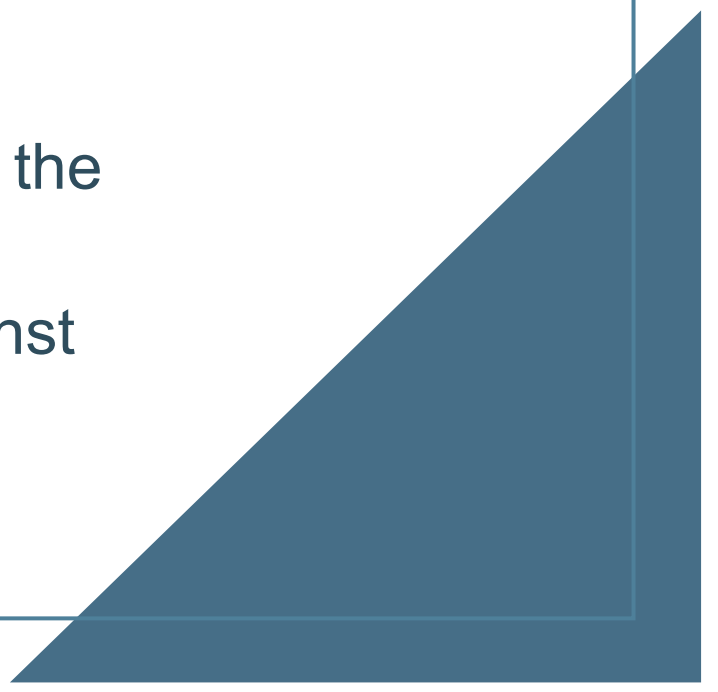
- CiTIP = Centre for IT & IP law, affiliated to a research group on security and privacy (imec)
 - Research unit of the Faculty of Law
 - Over 30 years of experience in conducting research in the legal and ethical aspects of innovative technologies
 - More than 80 full-time researchers involved in interdisciplinary projects funded by European and national programmes
- 

Research focus

Marie Curie postdoctoral fellowship
on facial recognition use in public
spaces for surveillance purposes

- Research on the impact on the EU rights to privacy and data protection
- Comparative analysis based on 4 countries
- Technical analysis in cooperation with technical experts

Overview

- Context
 - Functioning of the platform
 - Data Protection issues: Clearview AI / LEAs in the EU
 - Overview of legal actions and complaints against the company
- 

CONTEXT



The New York Times

The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and “might lead to a dystopian future or something,” a backer says.

Article of 18 January 2020



Facts

In its investigation published on 18 January 2020, **The New York Times** revealed the practices of a facial recognition software company, Clearview AI, based in the USA.

“

His tiny company, [Clearview AI](#), devised a groundbreaking [facial recognition](#) app. You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared. The system — whose backbone is a database of more than three billion images that Clearview claims to have scraped from [Facebook](#), YouTube, Venmo and millions of other websites — goes far beyond anything ever constructed by the United States government or Silicon Valley giants. ”

Extracted from NYT's article

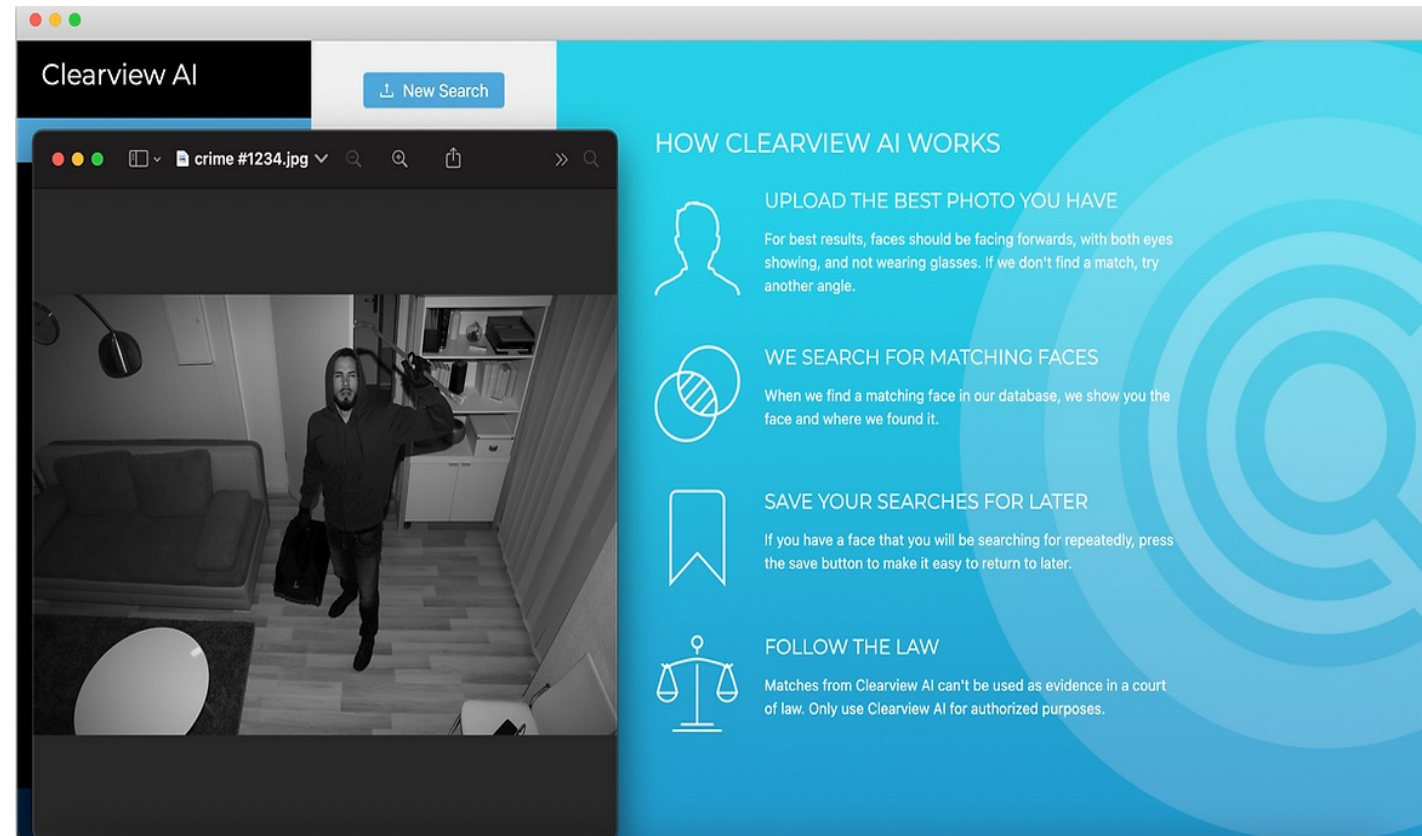
Update, 4 Oct. 2021: according to Clearview's founder, the company has now more than 10 billion images in its database
Source: Will Knight, 'Clearview AI has New Tools to Identify You in Photos' (Wired)

FUNCTIONING



STEP 1: Uploading an image

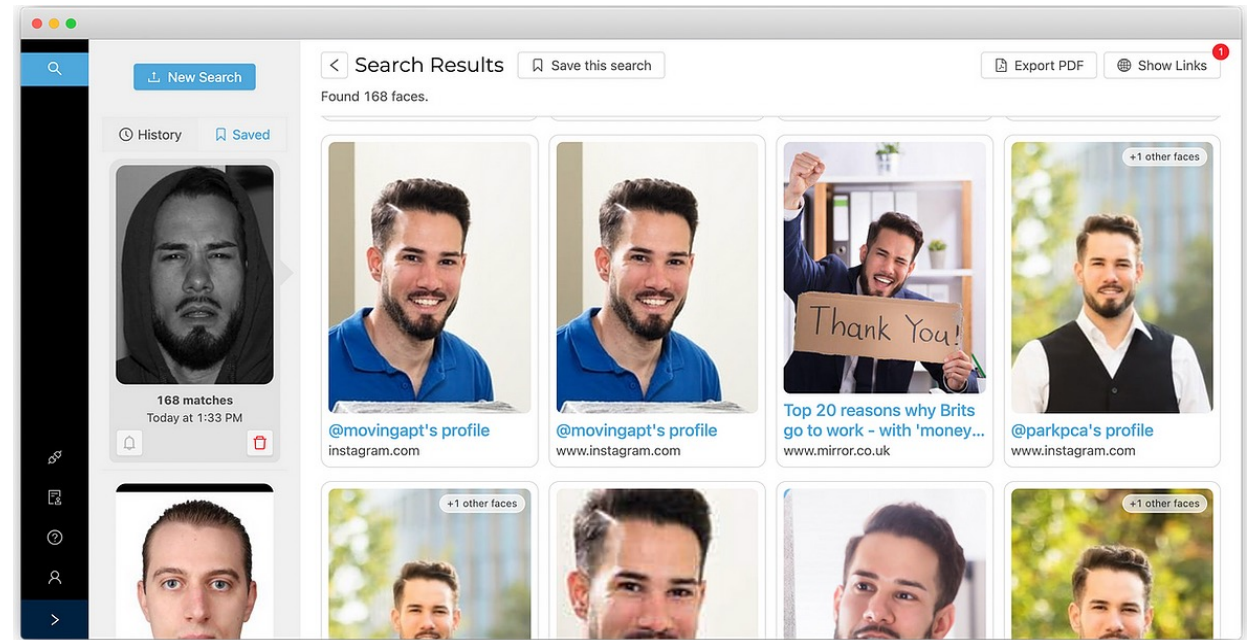
“Image is uploaded and required intake form (case number and crime type) is completed”



Credit photo/text = Clearview AI

STEP 2: Searching through the facial recognition database

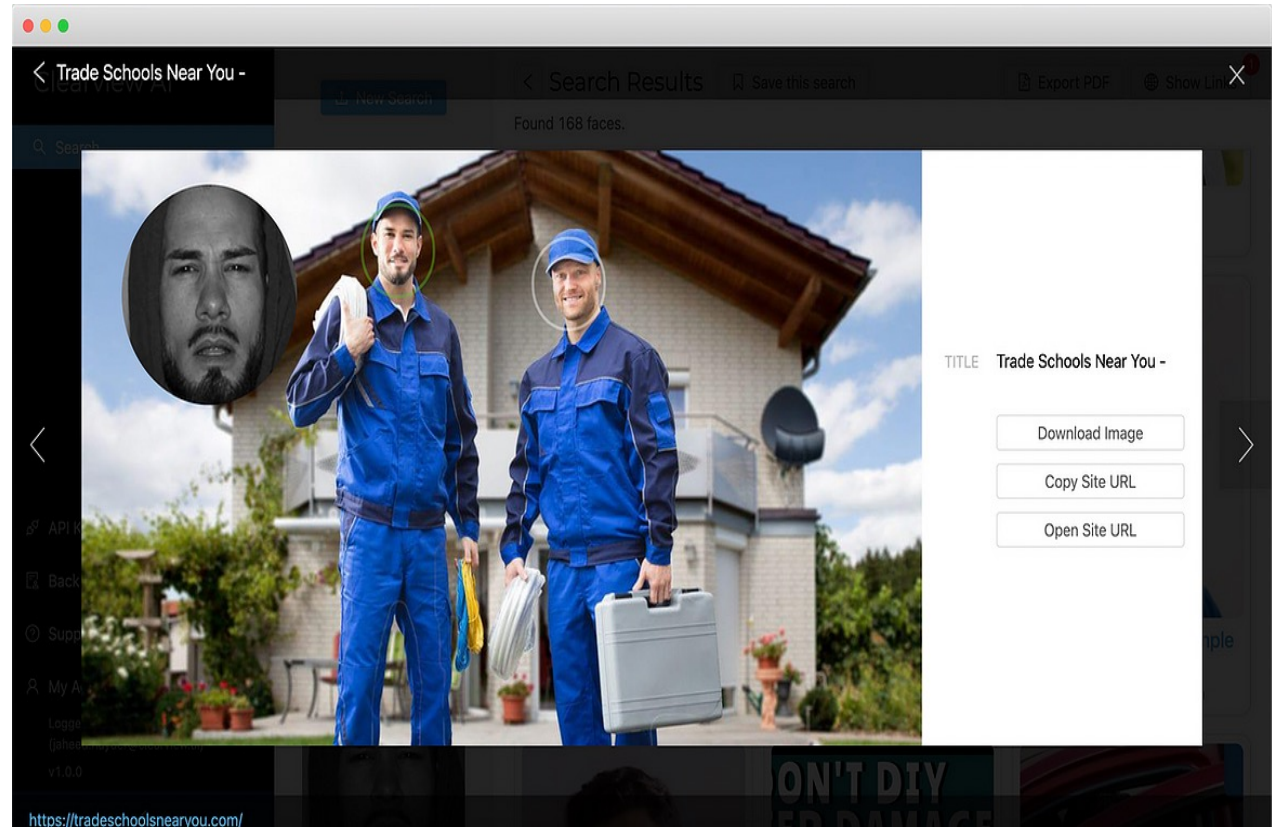
“Clearview AI searches probe against images indexed from public web sources and custom galleries”



Credit photo/text = Clearview AI

STEP 3: Matching

“Facial image results are returned with a source URL for public images”



Credit photo/text = Clearview AI

STEP 4: Results

“End user should verify and support returned results with further investigative steps”

Face Search Results

Disclaimer: In order to complete your request, we have generated this report containing Clearview search results for the image that you shared with us, which is labelled "Original Search Image" below. Search result images are enumerated with corresponding public web page titles and URLs below.





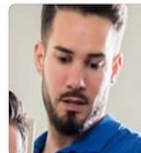






Image Index

1. @elmundotoday's profile. <https://www.instagram.com/p/BSiE30IFIKQ>
2. @valetparkingllc's profile. <https://www.instagram.com/p/Bp0lwLNA041>
3. 8 Retail Window Cleaning Tips and Tricks - FBM-Web. <https://www.focuscleaning.ca/8-retail-window-cleaning-tips-and-tricks/>
4. Helpful tips for an Air Force DITY PCS Move - Simple Moving Labor. <https://www.simplemovinglabor.com/helpful-tips-for-an-air-force-dity-pcs-move/>
5. Trade Schools Near You -. <https://tradeschoolsnearyou.com/>
6. @washingtoncourtdc's profile. <https://instagram.com/p/Bt6lFmXhzgs>
7. @quickserve_relocations's profile. <https://www.instagram.com/p/CHpEL98Jtsx>

Credit photo/text = Clearview AI

Technical description of the tools (based on NOYB's complaint)

1. Clearview AI uses an '**automated image scraper**' to search the Internet and collect images where it detects human faces + 'metadata' (information associated with the images) – all stored on Clearview AI's servers
2. **Facial features** are then **extracted** through image processing

'for each image collected, every face contained in the image is scanned and processed in order to extract its uniquely identifying facial features. Faces are translated into numerical representations which [NOYB] refer(s) to as "vectors". These vectors consists of 512 data points that represent the various unique lines that make up a face.'

Technical description of the tools (based on NOYB's complaint)

3. Clearview AI **stores vectors** in a database (associated with images and other info) – The vectors are then **hashed** for indexation and future identification purposes.
4. When a user uploads a picture, the platform analyses the image, extracts the features and hashed them to **compare** them against existing hashed vectors. Matching images will be shown to the user.

* For more details, see complaint by NOYB to the Austrian Data Protection Authority and by PI to the UK Data Protection Authority (ICO)

DATA PROTECTION ISSUES

Data Protection Issues

1. After the New York Times' revelations, **several legal complaints and actions** were initiated in Europe (before several data protection authorities) and outside Europe (Canada, Australia, and legal proceedings in California and Illinois) for violation of data protection and privacy legislation.
2. Focus on the EU data protection framework, but other privacy legislation could be analysed.
3. Distinction between the **Clearview AI's practices** and the **law enforcement authorities' use of the tool**.

Data Protection Issues

EU data protection framework composed of:

1. A general instrument (**General Data Protection Regulation**/GDPR)
 - ▶ Applicable to Clearview AI's practices? (issue of territoriality)
2. A specific instrument in the field of law enforcement (**Law Enforcement Directive**/LED) that needs to be implemented at national level
 - ▶ national rules applicable to law enforcement authorities using Clearview AI's tool

Clearview AI's practices / GDPR

1. Territorial scope of the GDPR: under which conditions can the GDPR apply outside the EU?
2. Nature of the data collected by Clearview AI?
3. Which principles and rights does Clearview AI most likely infringe?

Scope of the GDPR

Art. 3 GDPR

Main rule: GDPR applies to the controllers (entities in charge of the processing) and processors (entities acting on behalf of controllers) that have an establishment in the EU (Art. 3(1) GDPR)

But in the absence of establishment, the GDPR applies to entities either :

- 1. Offering goods and services to individuals in the EU or**
 - 2. Monitoring their behaviour as far as their behaviour takes place in the EU**
- (Art. 3(2) GDPR)

Scope of the GDPR / Clearview

Clearview AI does not have an establishment in the EU, is not offering services or goods to data subjects (?), but is it **monitoring the behaviour of data subjects in the EU?**



Individuals must be ‘targeted’ in the EU

≠ place of residence

= location of data subjects and monitored behaviour
(cumulative conditions)

Ex. tracking a person on the internet through cookies,
behavioural studies based on individual profiles...

*** EDPB’s Opinion 3/2018 on on the territorial scope of the GDPR**

Scope of the GDPR / Clearview

Based on Hamburg Data Protection Authority's Order, Clearview AI monitors the behaviour of data subjects in the EU:

- The company records the behaviour of individuals and stores it in the form of personal data.
- The **purpose of the tool is to identify individuals**, thanks to the recording/storage of publication/profiles/accounts of users linked to a photograph to create a profile of an individual.
- The company archives pictures over time.
- In the case before Hamburg data protection authority, the complainant was also physically present in the EU when he accessed the Internet.

Nature of the data

1. ...The data (images and associated information) collected and processed by Clearview AI are **personal data, biometric data, and sensitive data**

Personal data: 'any information relating to an identified or identifiable individual' (Art. 4(1) GDPR)

- Photographs scraped from the internet
- but also other information collected (webpage where the photographs are found, titles, etc) = info that can be used to indirectly identify the individual

Nature of the data

1. ...The photographs collected by Clearview AI are processed to be used for biometric identification purposes

Biometric data = personal data ‘resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as **facial images**’ (Art. 4(14) GDPR)

Rec. 51: photographs become biometric data when they are processed to ‘allow the unique identification or authentication’ of a natural person.

Nature of the data

2. Besides being personal data, the photographs transformed into biometric data are also sensitive data

Art. 9 GDPR provides a higher level of protection for sensitive data (such as data relating to health, ethnicity). The exhaustive list includes 'biometric data for the purpose of uniquely identifying a natural person.'

In conclusion: photographs collected from online sources (≠ biometric data, but can be sensitive data if reveal sensitive information) but as soon as they are processed for identification purposes = biometric data and sensitive data

Data Processing Principles

1. ...Images (and associated information) collected are **neither 'publicly available'** (the websites from which they were scraped are accessible but not publicly available) **nor freely re-usable**.
2. Clearview AI's practices most likely **infringe** the principles of **transparency, lawfulness, fairness**, but also **purpose limitation** and **data subjects' rights** (such as the right to information).

Data Protection Principles

1. ...According to the principle of transparency, individuals should be notified that their data were processed, which is not the case.
2. ...Fairness means that the processing is in line with individuals' reasonable expectations of privacy...it is hard to argue that individuals publishing photographs of themselves (or third-parties) would expect their images to be processed for identification purposes, including for police purposes.
3. Lawfulness means that the processing must comply with one of the legal grounds to process personal data (Art.6 GDPR) and sensitive data (list of exceptions in Art. 9(2) GDPR)).

Data Protection Principles/legal grounds

1. It is obvious that Clearview AI did not rely on consent to scrap the images.
2. Other legal bases to process personal data do not seem adequate as well:

for ex, **Art. 6(1)(f)** provides that the processing is necessary for the legitimate interests of the controller.

This is the legal ground that Clearview AI mentioned in a previous version of its privacy policy

Not convincing b/c : interest is purely commercial, some data are sensitive data, such processing is not in line with individuals' expectations concerning the use of their data...

Data Protection Principles/ legal grounds

1. Concerning the processing of sensitive data (which includes the processing of photographs for biometric purposes), Clearview AI argued that the data were publicly available.

Art. 9(2) (e) GDPR provides for an exception to process sensitive data when the data have been made manifestly public by the data subjects themselves.

Not convincing b/c: the exception has to be interpreted narrowly, i.e. the individuals themselves must disclose voluntarily the data and they should expect the further use...

LEA's use

On **25 August 2021**,
BuzzFeed News
released an
investigation it
conducted on law
enforcement and
government agencies
that used/tried the tool
provided by Clearview
AI

“ Clearview AI’s business model, which scoops up photos of billions of ordinary people from across the internet and puts them in a perpetual police lineup, is a form of mass surveillance that is unlawful and unacceptable in our democratic, rights-respecting nation” according to the director of the Canadian Civil Liberties Association (Brenda McPhail)

Extracted from BuzzFeed.News Investigation
'Police in at least 24 countries have used Clearview
AI. Find out which ones here'
:<https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table>

Law Enforcement Authorities' use

1. Are law enforcement authorities allowed to use Clearview AI's tool in the EU?
2. The Swedish Data Protection Authority issued a fine equivalent 250 000 Euros against the police for unlawful processing and failure to conduct a Data Protection Impact Assessment.
3. The EDPB made an initial assessment regarding the Clearview AI app and its use by law enforcement authorities in the EU.

Law Enforcement Authorities' use

The EDPB raised several issues:

- The **legality of the processing**:

Art. 8 LED provides that the processing can only be carried out if necessary for the performance of a law enforcement task based on law

Besides, to process sensitive data (including biometric data), Art. 10 LED requires that the processing is strictly necessary and subject to safeguards

- The use would also imply the **sharing of personal data outside the EU** with a private party to compare data against a 'mass and arbitrarily populated database of photographs'

Serious doubts about the existence of national or EU law for such processing

OVERVIEW LEGAL ACTIONS/COMPLAINTS

LEGAL COMPLAINTS in Europe

1. Hamburg Data Protection Authority's order:

- Request to delete the hash value generated for the complainant.
- Order limited in scope (only one individual) and no request to delete the images captured from the website for this individual.

2. Decision by the Swedish Data Protection Authority against police's use

3. **Complaints under review** led by Privacy International (before the French and UK data protection authorities), NOYB in Austria, Homo Digitalis in Greece, Hermes Centre for Transparency and Digital Human Rights in Italy

- ▶ coordinated action, coordinated answer from all the data protection authorities?

LEGAL COMPLAINTS in Europe

As summarised on EDRI's website, they argue the following

- The Regulation (EU) 2016/679 (General Data Protection Regulation) ("GDPR") applies to Clearview's collection and biometric processing of faces found online, as these consist in mass processing of European residents' personal data;
- Clearview processes both "regular" personal data (Article 4(1) GDPR) and sensitive or "special categories" data (Article 9(1) GDPR);
- Clearview has no lawful basis for collecting and processing any of this data. In particular, it does not obtain data subjects' consent and such practices cannot fall under its "legitimate interests". In addition, the processing of special categories data cannot be considered to be of data that has been "manifestly made public" by the data subject (Article 9(2)(e) GDPR);
- Clearview contravenes a number of other GDPR principles, including the principles of transparency (Article 5(1)(a) GDPR) and purpose limitation (Article 5(1)(b) GDPR);
- The use of Clearview's tool by law enforcement authorities does not fulfil the conditions for law enforcement processing required by the Law Enforcement Directive (2016/680) as transposed in EU member states' national laws. The use of such an invasive, privately developed facial recognition database enabling social media intelligence by law enforcement would not be based on law, nor would it be necessary and proportionate.

LEGAL COMPLAINTS outside the EU

1. Joint decision by Privacy commissioner of Canada and provincial authorities

- Clearview AI in breach with privacy legislation (collection without consent)
- Order to stop offering the tool to clients in Canada, stop collection/use/disclosure of images and biometric data collected from individuals in Canada, and delete images and biometric data already collected.

2. Decision by the Australia's Information and Privacy Commissioner:

- Clearview AI has breached the Australian Privacy Act for collecting sensitive info without consent, collecting personal information with unfair means, not notifying individuals, not ensuring the accuracy of the information, and not implementing practices, procedures and systems to comply with the Australian Privacy Principles
- Clearview AI should stop collecting images and templates from individuals in Australia and delete existing ones.

Investigation on-going concerning police's trial of the tool.

LEGAL COMPLAINTS outside the EU

1. In the **USA**, Clearview was sued by ACLU in Illinois for violation of the Illinois Biometric Privacy Act (covers private companies)

As a consequence, Clearview AI stopped selling its product to private companies in the USA.

2. Lawsuit by in Vermont for collecting photographs without consent (on-going)

3. Lawsuit by civil liberties activists in California for 'widespread collection of California residents' images and biometric information without notice or consent.' (on-going)

Food for Thought

- Little doubt that Clearview AI's practices are unlawful
- But despite the ongoing actions against the company, it still develops its business and holds even more images
- Besides privacy/data protection issues, such practices threaten the open Internet...



**This research and presentation was
funded by the MSCA-IF 895978
DATAFACE project, an EU Horizon 2020
research and innovation programme**

Thank you for your attention !
Q & A

catherine.jasserand@kuleuven.be