Special Issue Article

NJECL

New Journal of European Criminal Law
2020, Vol. 11(3) 375–389

DOI: 10.1177/2032284420948161
njecl.sagepub.com
SAGE

Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective

Isadora Neroni Rezende
Universitat Autònoma de Barcelona, Spain; Università di Bologna, Italy; Katholieke Universiteit Leuven, Belgium

Abstract
Since 2019, over 600 law enforcement agencies across the United States have started using a groundbreaking facial recognition app designed by Clearview AI, a tech start-up which now plans to market its technology also in Europe. While the Clearview app is an expression of the wider phenomenon of the repurposing of privately held data in the law enforcement context, its use in criminal proceedings is likely to encroach on individuals' rights in unprecedented ways. Indeed, the Clearview app goes far beyond traditional facial recognition tools. If these have been historically limited to matching government-stored images, Clearview now combines its technology with a database of over three billion images published on the Internet. Against this background, this article will review the use of this new investigative tool in light of the European Union (EU) legal framework on privacy and data protection. The proposed assessment will proceed as follows. Firstly, it will briefly assess the lawfulness of Clearview AI's data scraping practices under the General Data Protection Regulation. Secondly, it will discuss the transfer of scraped data from the company to EU law enforcement agencies under the regime of the Directive 2016/680/EU (the Directive). Finally, it will analyse the compliance of the Clearview app with art 10 of the Police Directive, which lays down the criteria for lawful processing of biometric data. More specifically, this last analysis will focus on the strict necessity test, as defined in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. Following this assessment, it will be argued that the Clearview app's use in criminal proceedings is highly problematic in light of the EU legislation on privacy and data protection.

Keywords
Facial recognition, data protection, privacy, surveillance, GDPR, Directive 2016/680/EU

Corresponding author:
Isadora Neroni Rezende, Università di Bologna, Dipartimento di Scienze Giuridiche, Via Zamboni 27/29, 40126 Bologna, Italy.
E-mail: isadora.neroni2@unibo.it

Introduction

At the beginning of 2020, a *New York Times* report[1] put a once little-known start-up, Clearview AI, under the spotlight. According to the report, this mysterious tech company had admitted selling a new facial recognition app to over 600 law enforcement agencies across the United States. Nothing new under the sun, one could argue: police have been using facial recognition for a while now. However, the Clearview app goes far beyond traditional facial recognition tools. If these have been historically limited to matching government-stored images (ie mugshots, driver's licence photos), Clearview now combines its technology with a database of three billion images published on the Internet. Clearview's engineers have designed software that can automatically collect people's photos from a variety of websites ranging from employment to news and education, as well as targeting social networks, such as Facebook, YouTube, Twitter, Instagram and LinkedIn. This practice, going under the name of data scraping, is undoubtedly controversial from a privacy standpoint. Unsurprisingly, the 'Clearview case' has prompted an outbreak of worldwide criticism from human rights advocates.[2] Social network companies, such as Twitter and YouTube, have also sent cease-and-desist letters demanding Clearview to stop data scraping from their websites.

On the other hand, Hoan Ton-That, Clearview's founder and CEO, has defended the lawfulness of the company's data processing practices, as well as the accuracy of its facial recognition technology. He further highlighted that the Clearview app has been crucial in solving many cases involving shoplifting, identity theft, credit card fraud, murder, terrorism and child exploitation.[3] From a general perspective, the Clearview case clearly falls within the global trend of reuse of data collected by the private sector for law enforcement purposes.[4] Many transparency reports are now showing that law enforcement agencies are increasingly asking to access data stored by tech giants such as Facebook, Google and Microsoft. In many instances, government agencies have even begun purchasing personal data from private companies to circumvent legal safeguards surrounding law enforcement access to commercial databases (ie subpoenas or judicial warrants).[5] However, the Clearview case differs from other scenarios involving the disclosure of personal data from the private sector to law enforcement: personal data are not transferred to police forces on a case-by-case basis, against payment or pursuant to a legal obligation, but they are collected by a private company with the precise intent of making them available, through an institutional arrangement, to government agencies for policing purposes.

1. Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' *New York Times* (18 January 2020, New York) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> accessed 4 March 2020.
2. Orsolya Reich, 'Clearview AI – The Privacy-Breaching App That Gives Us the Creeps' *EU Liberties* (14 February 2020) <https://www.liberties.eu/en/news/clearview-privacy-busting-app/18762> accessed 5 March 2020.
3. Andrew Tarantola, 'Why Clearview AI is a threat to us all' *Engadget* (12 February 2020) <https://www.engadget.com/2020/02/12/clearview-ai-police-surveillance-explained/> accessed 5 March 2020.
4. On the convergence between public and private databases, see Andrew Guthrie Ferguson, 'Big Data Surveillance: The Convergence of Big Data and Law Enforcement' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (CUP, Cambridge 2017). See also Valsamis Mitsilegas, 'The Transformation of Privacy in an Era of Pre-Emptive Surveillance' (2015) 20 *Tilburg Law Review* 35.
5. Sarah Brayne, 'Big Data Surveillance: The Case of Policing' (2017) 82 *American Sociological Review* 977, 995.

As Clearview AI (Clearview) plans to sell its technology also to European law enforcement agencies,[6] there emerges a pressing need to assess the impact that this disruptive facial recognition tool may have on individuals' rights in criminal proceedings. Different European Union (EU) Member States are indeed starting to test or rely on real-time facial recognition systems, giving rise to several societal concerns, as acknowledged by some EU institutions.[7] The need for a careful legal analysis of these issues also arises from the complexity of the EU data protection framework, which comprises two distinct instruments: on the one hand, the Regulation 2016/670/EU (the General Data Protection Regulation (GDPR)),[8] applicable to data processing operations for commercial purposes; on the other, the Directive 2016/680/EU (the Directive),[9] which regulates data processing in the law enforcement context.

Against this background, this article will investigate whether the use of the Clearview app in criminal investigations is compliant with the EU privacy and data protection framework. Firstly, we will briefly assess the lawfulness of Clearview's data scraping practices under the GDPR. Secondly, we will discuss the use of scraped data by EU law enforcement agencies under the regime of the Directive. In particular, this analysis will revolve around the role that Clearview would acquire, pursuant to the Directive, in the data processing within the framework of partnership agreements concluded with law enforcement agencies across the Union. Finally, we will assess whether the Clearview app abides by the criteria set out in art 10 of the Directive on lawful processing of biometric data. In this last step, we will focus on the strict necessity test, as defined by the Charter of Fundamental Rights of the European Union (the Charter) and the European Convention on Human Rights (ECHR).

Clearview's data scraping activities under the GDPR

Generally speaking, data scraping is a broad expression describing 'a plethora of internet-based data-retrieval methodologies from vast and various sources, collected *without* the website owner's consent'.[10] Unfortunately, the privacy and data protection issues raised by data scraping activities have not been analysed in detail within the literature. In our specific case, the assessment of these particular data processing operations requires us to answer a preliminary question, aimed at identifying the applicable EU legal instrument. As we already pointed out, the EU data protection framework is composed of two distinct instruments: a general one, whereas the other is focused on data processing performed by law enforcement authorities for the purpose of tackling crime.

6. See Samuel Stolton, 'After Clearview AI scandal, Commission "in close contact" with EU data authorities' *Euractiv* (12 February 2020) <https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/> accessed 5 March 2020.
7. Commission, 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust' COM(2020) 65 final, 22; European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (27 November 2019) 17–18.
8. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
9. Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.
10. Fiona Campbell, 'Data Scraping – What Are the Privacy Implications' (2019) 20 *Privacy & Data Protection* 3.

Determining the applicable instrument in this case is not a trivial question, if we look at the *material* and *territorial* scope of the two regimes.

On the applicability of the GDPR or the Directive

When dealing with the material scope of the two frameworks, we first need to assess whether Clearview collects people's publicly available images to satisfy a purely economic interest, or to perform a law enforcement operation entrusted by the competent authorities. Only in the latter case indeed, data scraping activities would be excluded from the scope of the GDPR, pursuant to art 2(2)(d),[11] thereby falling within the scope of the Directive. At this initial stage, it is safe to argue that the company itself does not engage in preventive or investigative activities, *on behalf* of any public authorities operating in the law enforcement context.[12]

This assertion is reinforced when read in conjunction with Clearview's privacy policy.[13] In fact, in stating the purposes of its data processing activities, Clearview indicates that it

> collects publicly available images and *shares* them, along with the source of the image, in a searchable format with our users, who are all law enforcement, security and anti-human trafficking professionals in the United States. This enables *users* to: facilitate law enforcement investigations of crimes; investigate and prevent fraud and identity theft. (emphasis added)

From the wording of the privacy policy, it is clear that Clearview's practices are primarily motivated by an economic interest, meaning that the company collects data to commercially exploit their value and provide its services to law enforcement agencies. Certainly, data collection is exclusively aimed at tackling crime in the law enforcement sector; however, Clearview does not act here as a competent authority within the meaning of the Directive. Data collection is first motivated by Clearview's interest in sharing – a more appropriate label would be describing it as *selling* – gathered data with its *users* (ie police agencies), those who are directly involved in the investigation of criminal offences. This means that, although data collection is performed *to the benefit* of law enforcement, it is not done in the exercise of a delegated public power, as required by art 3(7)(b) of the Directive.[14] Taking all of this into account, we can conclude that Clearview's data scraping practices are performed to benefit law enforcement, while primarily serving the company's commercial objectives. Therefore, they fall within the material scope of the GDPR,[15]

11. Article 2(2)(d) GDPR is complemented by art 1(1) of the Directive, which limits the scope of the Directive to personal data processing performed by law enforcement authorities for the purposes of preventing, investigating, detecting, prosecuting criminal offences and executing criminal penalties. Still, the Regulation does not exclude from its scope *all* data processing for law enforcement purposes, which are explicitly mentioned at art 23 GDPR. Hence, data transfers from private parties not acting as competent authorities to law enforcement agencies generally fall within the scope of the Regulation.
12. For the opposite scenario, where private citizens take part in law enforcement activities through a police-designed app, see Jonida Milaj and Gerard Jan Ritsema van Eck, 'Capturing Licence Plates: Police-Citizen Interaction Apps From an EU Data Protection Perspective' (2020) 34 *International Review of Law, Computers & Technology* 1.
13. Clearview AI, 'Privacy Policy' *Clearview AI, Inc.* (29 January 2020) <https://staticfiles.clearview.ai/privacy_policy.html> accessed 31 May 2020.
14. Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public–Private Partnership' (2018) 8 IDPL 52, 64.
15. Ibid 63: 'The only type of processing for the law enforcement purposes that is definitely excluded from the scope of the GDPR is by competent authorities'.

while the Directive (and national legislation implementing it) cannot be considered applicable at this stage.

Shifting the analysis to the territorial scope of the GDPR, different scenarios shall be taken into consideration. Firstly, the applicability of the Regulation needs to be assessed through the lens of the 'establishment' criterion, set out in art 3(1) GDPR.[16] Pursuant to this provision, the Regulation applies to personal data processing in the context of an establishment of a controller or a processor in the Union, regardless of where the processing takes place. If Clearview were to offer its services to law enforcement agencies in EU Member States, it would be highly probable that Clearview would establish itself in at least one EU Member State to better oversee its marketing operations in Europe. Here, the presence of a single employee or agent of Clearview might be enough to trigger the application of the GDPR, if the company's representative(s) acted with sufficient stability.[17] The EU local establishment would not be required to take any role in the data processing, insofar as its activities could be considered as being 'inextricably linked' to such processing.

Secondly, even if Clearview decides to not set up an EU office, its processing operations could still fall within the scope of the Regulation, according to the so-called 'targeting' criterion. If their data processing activities were related to the monitoring of data subjects in the Union, the GDPR would apply as far as the targeted behaviour also takes place within the Union (art 3(2)(b) GDPR).[18] The meaning of this provision is further clarified in Recital 24 of the Regulation, which reads:

> in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including *potential subsequent* use of personal data processing techniques which consist of *profiling* a natural person, particularly in order to *take decisions* concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes (emphasis added).

Although the use of the Clearview app is mainly directed at the *identification* of individuals involved in criminal investigations taking place in EU Member States, its processing activities may also involve *tracking* individuals, who are in the Union. First, the images retrieved by the AI system are presented with their sources, that is, a link redirecting the user to the website storing the data. Of course, this also allows law enforcement – at a later stage – to track the online behaviour of people subject to monitoring, thus profiling them with the aim of detecting their preferences and habits, but also their location and movements.[19] Moreover, as images are mainly scraped in social media, they can also assist investigators in reconstructing a detailed picture of one's personal life. Indeed, social media pictures come with a great deal of contextual elements (eg background, company, location) from which sensitive information on the data subject can be inferred. Metadata

16. The notion of establishment is provided at Recital 22 GDPR. Although we cannot go into the specifics of the establishment criterion, we should note that the European Data Protection Supervisor (EDPS) has clarified that the threshold for the identification of a 'stable arrangement' can be quite low when the controller's centre of activities concerns the provision of online services. See EDPS, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation' (16 November 2018), at 4–12. Before the Regulation, the criterion was interpreted extensively by the CJEU in the *Google Spain* judgment, Case C-131/12 *Google Spain* ECLI: EU: C:2014:317, paras 50–53.
17. See EDPS (n 16) 5.
18. The targeting criterion is generally regarded by legal scholarship as a useful tool to expand the scope of GDPR. See Benjamin Greze 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) 9 IDPL 109, 110–14.
19. For the definition of profiling, see Recital 71 GDPR.

associated with the pictures can also play a role in ascertaining the potential location of an individual.

Therefore, it is possible to conclude that Clearview may engage in processing activities related to the monitoring of data subjects in the Union within the meaning of art 3(2)(b) GDPR; thus, the Regulation would apply to its data scraping operations, even if they did not take place in the Union.

Assessing sensitive data scraping under art 9 GDPR

Having established the (potential) applicability of the GDPR, the lawfulness of data scraping practices under the EU data protection regime shall be assessed. As the processing operations mainly concern a special category of personal data, the analysis will revolve around the stricter requirements laid down in art 9 GDPR.[20] In its privacy policy, Clearview explicitly states that their collection of facial images is grounded on their public availability on the Internet. Such operations may seem to be compliant with art 9 GDPR, which allows data controllers to process special categories of data 'which are manifestly made public by the data subject'. Actually, the issue may be more complex than it first appears. Indeed, the meaning of the expression 'publicly available' has not been fully clarified in the Regulation, nor in the literature.[21] Still, some considerations may be put forward when assessing the Clearview app. In this case, the analysis will exclusively focus on social media websites, as they represent the main source of data for the system's search engine.

When private companies scrape data from social media, they still need to comply with the policies of the targeted websites. To understand whether a site allows for web-scraping, its robots.txt file shall first be checked. The file can be accessed by adding '/robots.txt' right at the end of the link of the concerned website.[22] As we perform this rather simple procedure, we observe that most social media websites do not allow for data scraping, unless written permission is issued. Unsurprisingly, all major social media platforms have already sent cease-and-desist letters to Clearview, demanding that they stop all data scraping activities in their domains.[23]

Furthermore, data scrapers need to also respect individuals' privacy settings. Social media websites usually give users the option to choose the people with whom they want to share the details of their daily lives. Therefore, a picture cannot be considered as being 'publicly available' only because it was posted on social media.[24] For instance, when a picture is published on a private

20. See Recital 51 GDPR. At this stage, it might not be clear whether facial images – if being merely stored in Clearview's databases – could qualify as biometric data. To be considered biometrics, the image should be processed by an algorithm transforming the analogue information into digital information (data) based on the person's facial features. However, such images could still be treated as a *special category of personal data*, revealing the ethnic origin of a natural person, or potentially his or her religious beliefs, etc.
21. Kindt expresses some doubts on the meaning of the expression. See Els J Kindt, 'Having Yes, Using No? About the New Legal Regime for Biometric Data' (2018) 34 *Computer Law & Security Review* 523, 528.
22. Octoparse, '5 Things You Need to Know Before Scraping Data From Facebook' *Octoparse* (30 January 2019) <https://www.octoparse.com/blog/5-things-you-need-to-know-before-scraping-data-from-facebook> accessed 21 May 2020.
23. In response, Clearview invoked its First Amendment right to scrape publicly available data, see Kaixin Fan, 'Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data' *JoltDigest* (25 February 2020) <https://jolt.law.harvard.edu/digest/clearview-ai-responds-to-cease-and-desist-letters-by-claiming-first-amendment-right-to-publicly-available-data> accessed 5 June 2020.
24. Conversely, as pointed out by the Working Party 29 (WP29), when the concerned person posts images on other kinds of publicly available websites, he or she is clearly willing to make the information available to the general public, and so potentially to law enforcement. Cf WP29, 'Opinion on Some Key Aspects of the Law Enforcement Directive (EU 2016/680)' (WP 258, 29 November 2017) 10.

profile, the data cannot be freely collected by the scraping company. In this case, the user did not intend to make his or her personal information available to the general public, and even less so to law enforcement. Nevertheless, such considerations seem to not inform the current functioning of the system. For example, in an extended interview with Clearview's CEO, a CNN journalist ran his producer's picture into the app, which found images from her Instagram profile, even though that account was private and accessible only to her followers.[25]

In the same interview, Hoan Ton-That reported a case in which the face of a child predator had been detected by the Clearview app in the background of a gym selfie posted by a third person on his social media. This case brings our attention to another scenario, which questions the 'public availability' of the images stored in the company's databases. In some instances, the pictures may not have been made public by the interested data subject; they could also have been taken in contexts, where the portrayed individual may have claimed to have a reasonable expectation of privacy. In all these cases, the legal basis set out in art 9(2)(e) GDPR cannot be seen as fulfilled, and data scraping operations should be considered unlawful.

Having examined how initial data scraping activities may violate the GDPR provisions, we will now analyse the scope of the Directive's application, which would regulate data sharing operations within the framework of partnership agreements between Clearview and EU law enforcement agencies.

Subsequent use of GDPR data in private–public partnerships

The relationship between the GDPR and the Directive undoubtedly sits on the penumbra of EU data protection law.[26] Indeed, even though certain provisions attempt to regulate the interrelationship between the two regimes, a significant degree of uncertainty still persists in the context of information sharing between private parties and law enforcement authorities.[27]

If private-to-public data transfers performed on a case-by-case basis are still subject to GDPR rules, the same cannot be said for information sharing schemes taking place in the framework of *structured* institutional arrangements between concerned parties.[28] Depending on the configuration of the agreement between private and public entities, two different scenarios need to be examined. On the one hand, Recital 11 of the Directive clarifies that when private entities or bodies are bound 'by a contract or other legal act' to law enforcement agencies, they process data *on behalf* of competent authorities and become *processors* under the Directive.[29] In this case, GDPR applies to initial data collection activities – as we have argued – and the Directive regulates data processing within the context of the public–private partnerships concluded by the company.

On the other hand, when the private and public parties determine the objectives of the processing *as equals*, Purtova contends that a situation of joint controllership is established.[30] Here, the

25. Donie O'Sullivan, 'This man says he's stockpiling billions of our photos' *CNN Business* (10 February 2020) <https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html> accessed 21 May 2020.
26. See, in that respect, also the contribution by Foivi Mouzakiti in the present volume.
27. Purtova (n 14) 62 (citing Gertjan Boulet and Paul de Hert, 'Cooperation Between the Private Sector and Law Enforcement Agencies: An Area in Between Legal Regulations' in Aden Hartmut (ed), *Police Cooperation in the European Union Under the Treaty of Lisbon* (Nomos, Baden-Baden 2015) 252.
28. Purtova (n 14) 65.
29. Recital 11 of the Directive.
30. Article 26 GDPR; art 21 of the Directive.

private entity fully acquires the status of being a 'competent authority' within the meaning of art 3(8) of the Directive, which could then also extend its applicability to previous data collection activities.[31]

In summary, the actual scope of the Directive shall be assessed here on a case-by-case basis, depending on the exact terms of the partnership agreement that could involve Clearview and the concerned law enforcement agency. The key determinant lies – as said – on the weight given to the company in setting the goals, limits and means of the processing within the private–public partnership. Although precise predictions are difficult to make, some hypothesis on the case at hand could still be postulated. For instance, to qualify as a joint controller, Clearview should have an actual power on *when* and *under which circumstances* processing activities are carried out in the context of real criminal investigations or pre-emptive operations. This means that the company should also be able to perform both the necessity and proportionality assessments, as any other law enforcement authority in real-time situations.[32] Setting aside the considerable legitimacy issues that such scenarios would give rise to, we suggest here that the current configuration of legal agreements concluded by Clearview in the United States could rule out a situation of joint controllership in the Union. From the available US reports, it appears that Clearview is acting as a simple provider of a facial recognition service to competent authorities. Thus, police officers are the ones who decide when to run a picture in the system in concrete cases. Conversely, there is no evidence in the news of Clearview refusing to match an uploaded image with those stored in its databases.

It appears like Clearview would become a processor under the Directive when providing its services to police departments under a stable partnership agreement. Although a situation of joint controllership cannot be completely discarded, such a scenario would certainly be the least desirable from a democratic perspective.

Assessing Clearview under art 10 of the Directive

Interestingly, facial images per se do not constitute biometric data under the EU data protection legislation.[33] According to art 3(13) of the Directive, data are considered to be biometric only if (a) they result from a *specific technical processing*, meaning that the mere storage of such data does not necessarily require the application of the specific regime; (b) they allow for the *unique identification* of a natural person. Thus, the initial data can hardly be considered biometric in itself; it is rather the use of specific means of processing to submit the data to this particular regime.

Pursuant to this legal definition, we contend here that the processing of facial images by Clearview – and potentially by criminal justice authorities of EU Member States – must be qualified as biometric data, and therefore be subject to the particular safeguards of art 10 of the Directive. As in our case, facial images are processed in the context of a criminal investigation, the biometric processing is clearly aimed at the identification of a precise individual. It is well-known that identification per se represents an unavoidable precondition of many (if not all) law

31. Purtova (n 14) 66.
32. Ibid 65.
33. Kindt provides a detailed analysis of the concept of biometric data in the GDPR and the Directive. See Kindt (n 21) 529–34. It should be noted, nonetheless, that facial images per se are covered by the protection of art 8 ECHR, see, eg, *von Hannover v Germany* ECHR 2004-VI 41, paras 76–78; *Peck v UK* ECHR 2003-I 123, paras 60–62; *Bogomolova v Russia* (App no 13812/09) ECtHR 20 June 2017, para 52.

enforcement activities.[34] Here, Clearview's processing concretely allows for such identification, as it matches facial images with social media profiles and websites that may easily lead to the identity of a data subject. Besides, facial images are here collected not for mere storage purposes; they are also processed for biometric comparison by an AI system, and therefore can be considered as being the result of a specific technical processing.[35]

Having qualified the data processed by the Clearview app as biometric, we should assess whether – or under which circumstances – the use of such tool may be compliant with the requirements set out in art 10 of the Directive.

Lawful processing

Article 10 of the Directive allows for the processing of biometric data only (a) where authorized by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; (c) where such processing relates to data which are manifestly made public by the data subject.

As for the first condition, the deployment of the Clearview app could be grounded either on EU or national legislation, specifically regulating the processing of biometric data for real-time identification purposes in the criminal justice sector. In particular, if biometric processing is based on Member State law, this should be allowed only when necessary to protect the vital interests of the data subject or another natural person, or when the data have manifestly been made public by the data subject.[36] If the second scenario has already been examined in the context of the present contribution,[37] the former may refer to situations where there is an immediate danger for the life and personal integrity of individuals (*eg* to prevent a terrorist attack), or a need to protect the vital interests of victims of serious criminal offences (*eg* in the case of human trafficking, child pornography).

Strict necessity test

Article 10 of the Directive allows for the processing of biometric data only when it is strictly necessary. For the purposes of this assessment, the strict necessity test – being an aspect of the broader principle of proportionality – should be interpreted in accordance with art 52(1) of the Charter, which is applicable within the scope of EU law. As we are dealing with an encroachment on the rights to privacy and data protection, we shall also refer to art 8(2) of the ECHR, which adds that any limitation to the rights at stake must be strictly necessary 'in a democratic society'. Even if the Charter uses a different wording, the *democratic society* requirement present in the ECHR is integrated into our analysis.[38] Accordingly, the case law of the European Court of Human Rights (ECtHR) will be taken into account when examining the strict necessity criterion.

34. Technically, there is a distinction between processing for the purposes of *identification* and *verification.* In the latter case, data are used in a one-to-one comparison to check whether an individual is the same person as the one from whom the biometric sample has originated, which does not require knowing the identity of the data subject.
35. On the difference between mere photographs and biometric data, see (n 21).
36. WP29 (n 24) 7.
37. See (n 26). All considerations made concerning the 'public availability' of facial images under GDPR are valid also in the law enforcement context.
38. The respect of democratic values is inherent in the EU legal order and it is mentioned at art 2 TEU. Also, art 52(3) of the Charter provides that, when the Charter protects rights corresponding to those guaranteed by the ECHR, the meaning and scope of such rights shall be interpreted as those enshrined in the Convention.

The content of the (strict) necessity principle has been clarified by the Court of Justice of the European Union (CJEU) in its *Schwarz* case:

> in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage *measures which will interfere less* with the rights recognised by Articles 7 and 8 of the Charter but will *still contribute effectively to the objectives* of the European Union rules in question.[39] (emphasis added)

In assessing the necessity of a limitation to the fundamental rights protected, the nature and the scope of the interference prompted by the measures taken by the authorities need to be evaluated first. In our case, different factors suggest that the interference with the rights to privacy and data protection may be particularly serious, thereby being subject to a more severe review.[40] Firstly, creating a database of three billion facial images for policing purposes clearly amounts to the creation of a blanket surveillance scheme, which means that citizens who do not have any connection whatsoever with criminal activities are likely to be put under screening by law enforcement. European supranational courts have highlighted the risks of unfettered surveillance, which is likely to engender in the minds of the people concerned a constant feeling of being monitored, stigmatized or treated as suspects with no apparent reason.[41] Furthermore, as biometrics allows authorities to uniquely identify citizens throughout the course of their entire lives, the indiscriminate collection of such data strongly undermines people's anonymity in public places. In turn, this may also impact on the exercise of other fundamental rights and freedoms, such as the freedom of expression, information and communication, or the freedom of assembly and association.[42] These risks may even be magnified for some vulnerable groups: indeed, the technology is often less accurate when it comes to identifying females and dark-skinned people,[43] as the design of facial recognition systems might still be affected by racial and gender biases. Overall, the deployment of this facial recognition tool, combined with an enormous database of privately collected images, seems to generate a significant limitation to people's rights to privacy and data protection. Hence, its use by law enforcement should be strictly regulated and monitored.

As said, the envisaged measure should not go beyond what is strictly necessary to fulfil the proposed objectives (in this case, the fight against crime). To satisfy this requirement, the assessment of the app shall focus on the existence of 'clear and precise rules governing its scope and application'.[44] Even if such rules were laid down in the European context, we argue here that the use of the Clearview app – as it stands today – would be highly problematic in the Union. While

39. Case C-291/12 *Schwarz v Stadt Bochum* ECLI: EU: C:2013:670, para 46. The *Schwarz* case is particularly relevant for the purposes of our assessment because it deals with the processing of biometric data (fingerprints) taking place in the framework of the Area of Freedom, Security and Justice.
40. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* ECLI: EU: C:2014:238, paras 47–48; *S and Marper v UK* [GC] ECHR 2008-V 167, para 102.
41. Cf *Digital Rights* (n 40) para 37; *Big Brother and Others v UK* (App no 58170/13, 62322/14 and 24960/15) ECHR 13 September 2018, para 225.
42. See, eg, Rina Chandran, 'Use of facial recognition in Delhi rally sparks privacy fears' *Reuters* (30 December 2019) <https://www.reuters.com/article/us-india-protests-facialrecognition-trfn/use-of-facial-recognition-in-delhi-rally-sparks-privacy-fears-idUSKBN1YY0PA> accessed 25 May 2020.
43. Steve Lohr, 'Facial Recognition is Accurate, if you're a White Guy' *New York Times* (9 February 2018, New York) <https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html> accessed 25 May 2020.
44. *Digital Rights* (n 40) para 54*; Rotaru v Romania* [GC] ECHR 2000-V 109, paras 57–59; *S and Marper* (n 40) para 99.

pointing out potential issues, we will also indicate how the use of the app may be circumscribed in some instances.

The main issue that comes with the adoption of the Clearview system concerns the size of its database, which contains – for the most part – images of people who have never been involved in criminal activities or with law enforcement. Since its *Digital Rights* judgment, the CJEU demands surveillance measures in the law enforcement context to be differentiated and restricted according to objective criteria presenting a link with the goals pursued.[45] With regard to the persons whose data are being retained, the use of the Clearview app seems to be significantly at odds with the requirements of the Court, and the contrast is probably irreconcilable. As strongly reiterated by the company's CEO, indeed, the force of the app lies in its capacity to search beyond government-based databases: its use, then, is overtly aimed at identifying people who would normally be far from the gaze of criminal justice authorities, and therefore could not be tied to the objectives of the fight against crime by any objective criterion.[46]

When applying the strict necessity test, one major question also concerns, *who* is going to be able to access the data. In our case, the use of the app should be governed by clear rules circumscribing the range of people authorized to access the data in the context of criminal investigations.[47] Due to the sensitivity of the data, the access to the software should be restricted to police officers having a certain grade or level of experience. Especially when the application is employed in its version for mobile devices, patrolling officers should be properly trained to recognize the situations where the real-time identification of an (suspect) individual may be adequate and proportionate. These decisions are particularly sensitive and should be made with extreme promptness.

As suggested above, the availability of the facial recognition tool for mobile devices, such as smartphones, is particularly relevant in our assessment. For instance, an indiscriminate use of the app by patrolling officers for real-time identification purposes may not align with the strict necessity criterion in most cases.[48] Indeed, in its Opinion on the application of the necessity principle in the law enforcement context, the Working Party 29 (WP29) stressed the importance of considering the precise circumstances in which the limitation of the rights at stake takes place. In particular, the unregulated deployment of data-driven investigative techniques can be questioned in situations where individuals may claim to have a certain expectation of privacy, even in public places.[49] With the Clearview app literally in police hands, the scope of urban surveillance may expand beyond the capacity of the tools already embedded in fixed infrastructure (ie CCTV), and

45. *Digital Rights* (n 40) para 57; Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* ECLI: EU: C:2015:650, para 93; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson and Others* ECLI: EU: C:2016:970, para 110; *Opinion 1/15* ECLI: EU: C:2016:656, para 191. Nonetheless, the ECHR seems to be taking a different approach, considering bulk interception of metadata to be per se compatible with art 8 of the Convention. See *Big Brother Watch* (n 41) para 314.
46. This issue has arisen also with respect to other kinds of government-based databases that were not originally set up for law enforcement purposes. See Kindt (n 21) 528.
47. *Digital Rights* (n 40) para 62.
48. Kindt expresses similar concerns regarding the continuous biometric comparison for identification purposes performed by smart CCTV cameras in public places. Cf Kindt (n 21) 528.
49. Cf WP29, 'Opinion 01/14 on the Application of Necessity and Proportionality Concepts and Data Protection Within the Law Enforcement Sector' (WP 211, 27 February 2014), at 10: '(. . .) the privacy considerations in terms of context are very different when installing CCTV cameras on a public street as opposed to installing them in toilets or hospital wards'.

take advantage of all kinds of mobile devices equipped with a camera. With no precise regulation on the matter, such a system of blanket surveillance may easily go beyond what is strictly necessary to tackle crime in the urban area, thus infringing citizens' rights to privacy and data protection in unnecessary ways.

Furthermore, the current functioning of the Clearview system seems to not comply with EU legislation in terms of data retention periods. For instance, art 5 of the Directive requires Member States to set appropriate time limits for the erasure of personal data or to establish a periodic review to assess the need for storing personal data. This provision is complemented by Recital 26, which emphasizes that personal data should not be kept for longer than necessary for the purpose for which they are processed. The CJEU also acknowledged the need to limit data retention periods in several cases,[50] in accordance with the case law of the ECtHR.[51] In the case at hand, Clearview's privacy policy does not provide any indication of the data retention period of facial images stored in the company's databases. It simply states that concerned persons have a right to have their data erased when the appropriate conditions are met.[52] It is not yet clear whether the company and concerned EU law enforcement agencies will establish precise time limits for data storage in their partnership agreements; for the time being, it seems that facial images stored in Clearview's databases will be kept there for an indeterminate period of time. Interestingly, this observation seems to be corroborated by an anecdote of a CNN journalist, who while uploading his photo in the Clearview app found a picture of him that had been published by an Irish local newspaper when he was 15 years old.[53] One could wonder what the interest of storing such old pictures could be. These may not properly reflect one's appearance anymore, and identification goals could be equally (or better) served by more recent pictures of the monitored subject. Actually, the accumulation of different (and maybe obsolete) images for the same person – associated with the relative sources – brings to surface the *tracking* purposes embedded in the system, which go beyond mere *identification* goals. In this perspective, the monitoring abilities of the system could be restrained only by clear rules, filtering the images that may be stored in the databases, and setting precise time limits for retention.

Finally, we should wonder whether the goals pursued by law enforcement in the Union could be achieved by less intrusive tools, which could still prove to be genuinely effective. As clarified by the European Data Protection Supervisor, not every measure that might be useful for certain purposes can be seen as 'desirable' or strictly necessary in a democratic society.[54] Furthermore, when the proposed measure involves the processing of sensitive data – as in this case – the threshold to be applied in the effectiveness assessment should be higher.

When thinking of the scope and intensity of urban surveillance, one could contend that the extensive use of CCTV cameras – although questionable under many ethical aspects – does already play a significant role in many criminal investigations.[55] Existing measures may thus be already

50. *Digital Rights* (n 40) paras 63–64; *Opinion 1/15* (n 45) paras 209–10.
51. *M.K. v France* (App no 19522/09) ECtHR 18 April 2013, paras 44–46; *Roman Zakharov v Russia* [GC] ECHR 2015-VIII 205, paras 254–55.
52. Clearview AI, 'EU/UK/Switzerland Deletion Request Form' <https://clearviewai.typeform.com/to/Icakh3> accessed 28 May 2020.
53. O'Sullivan (n 25).
54. EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (11 April 2017), at 17.
55. See, eg, Matthew PJ Ashby, 'The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis' (2017) 23 *European Journal on Criminal Policy and Research* 441.

satisfactory, or could be better implemented, while being less intrusive upon the rights protected. Privacy enhancing technologies are available for video surveillance to minimize the impact on citizens' private life (*eg* privacy masking). Alternatively, the deployment of facial recognition tools for law enforcement purposes may arguably be supported by a pressing need to fight particular forms of serious crime. In this case, however, the deployment of the technology would still need to be thoroughly circumscribed from a range of different angles. From this perspective, the systematic and unfettered use of social media pictures of people who have never been involved in criminal activities seems to put the Clearview app at irreconcilable odds with the requirements laid down by the CJEU in the field of surveillance.

Appropriate safeguards

A component of the broader proportionality test is the assessment of foreseen legal safeguards, which are key in counterbalancing the risks to fundamental rights of the envisaged surveillance measure.[56] The Directive requires that the processing of biometric data is surrounded by 'appropriate safeguards', which are also underlined in Recital 37: among them, there is the provision of 'stricter rules on the access of staff of the competent authority', which we have already examined.

According to the WP29, legal safeguards can also consist of additional substantial or procedural requirements accompanying the use of the tool.[57] Firstly, data processing should be restricted to the investigation and prosecution of a limited range of criminal offences. In *Digital Rights*, the CJEU examined this requirement in the context of the strict necessity test, considering that the mass data retention measure posed such a severe interference on the rights to privacy and data protection, but was limited to the fight against serious crime.[58] This means that, if the Clearview app were to be adopted by law enforcement agencies in Europe, its use could certainly not be extended to tackling forms of petty crime, such as pickpocketing.[59]

Secondly, from a procedural standpoint, the use of the software by law enforcement should be dependent on the prior review of a judicial or other independent authority, which would assess the strict necessity of the biometric processing in the concrete case.[60] Otherwise, the app could be exploited in situations of significant urgency (*eg* to prevent an imminent danger for the vital interests of many persons), but any access should then be subject to a review *a posteriori* by competent national authorities. Anyhow, the data subject should retain its right to have the outcome of the automated processing of his or her personal data reviewed by a human agent, as provided by art 11 of the Directive.[61]

Lastly, the implementation of the measure should be accompanied by additional data security measures,[62] ensuring the confidentiality and integrity of collected data. Here as well, news reports have cast doubts on the company's ability to protect its databases. In February 2020, Clearview

56. EDPS (n 54) 5.
57. WP29 (n 24) 8.
58. *Digital Rights* (n 40) para 60.
59. Cf *Zakharov v Russia* (n 51) para 244.
60. Cf *Digital Rights* (n 40) para 62.
61. Cf art 22 of the GDPR.
62. On data security, see arts 4(1)(f) and 29 of the Directive.

suffered a data breach that resulted in its entire customer list being stolen[63]; in April, hackers got access to the company's repository containing the app's source code, secret keys and credentials.[64] Although Clearview claims that its security standards are compliant with GDPR requirements, it will probably have to step up its game in terms of security, if it plans to market its technology in Europe.

Concluding remarks

Following our considerations, the use of the Clearview app by Member States' law enforcement agencies appears to be deeply problematic with regard to the rights to privacy and data protection, as protected in EU primary and secondary legislation.

As enshrined in art 7 of the Charter, privacy is traditionally conceived as a tool of *opacity*,[65] granting 'protection against arbitrary or disproportionate intervention by public authorities in the sphere of the private activities of any person'.[66] In turn, the right to data protection, which is designed in art 8(2) as a tool of *transparency*, legitimizes the processing of personal data insofar as the requirements laid down by law are satisfied.[67] Although distinct in their underlying logic, privacy and data protection share a strong conceptual link[68] and are both key in addressing data-driven forms of surveillance. As acknowledged by the CJEU in *Digital Rights* and *Tele2/Watson*,[69] both rights are instrumental to the exercise of other fundamental rights (*eg* the freedom of expression), which enable the flourishment of our constitutional democracies, and ultimately of our personal identity. The Court has repeatedly declared that even the objective of the fight against (serious) crime cannot, in itself, justify an indiscriminate collection and use of citizens' personal data in a democratic society,[70] as could happen in the Clearview case. That is why the CJEU will need to keep on enhancing the principle of proportionality[71]: only this way the asymmetries of power brought by opaque and pervasive surveillance schemes will be kept under constant review.

With regard to secondary legislation, we observed that bulk data scraping practices may violate GDPR provisions, as facial images cannot always be considered to have manifestly been made public by the data subject just because they were posted on social media. The same goes for when the data processing becomes subject to the rules of the Directive, namely once the company has concluded a partnership agreement with a law enforcement agency in the Union. In this context,

63. Betsy Swan, 'Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen' *DailyBeast* (26 February 2020) <https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen? source=twitter&via=desktop> accessed 29 May 2020.
64. Zack Whittacker, 'Security Lapse Exposed Clearview AI Source Code' *TechCrunch* (16 April 2020) <https://techcrunch.com/2020/04/16/clearview-source-code-lapse/> accessed 29 May 2020.
65. Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia, Antwerp 2006) 61–104, 62.
66. Case T-135/09 *Nexans v Commission* ECLI: EU: T:2012:596, para 40.
67. De Hert (n 65) 62.
68. Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* ECLI: EU: C:2010:662, para 47.
69. *Digital Rights* (n 40) para 28; *Tele2/Watson* (n 45) paras 93, 101.
70. *Digital Rights* (n 40) para 51; *Tele2/Watson* (n 45) para 103.
71. Article 52(1) of the Charter.

Clearview could acquire the status of being a processor pursuant to the Directive, while keeping its role as a controller under GDPR for initial data collection activities.

Even admitting the lawfulness of Clearview's data scraping initiatives in these limited instances, the subsequent use of these privately formed databases by law enforcement in the Union remains critical. Certainly, the deployment of the tool may be regulated in ways that would allow its use by police officers only in limited scenarios (*eg* for the investigation of serious criminal offences). However, the very reliance on such a large database of social media pictures, available *in bulk* to law enforcement, may be at odds with the requirements of the CJEU. It is one thing to use publicly available data of a particular data subject, which can certainly be searched for and accessed by law enforcement for investigative needs. Another is to provide, all at once, law enforcement agencies with an enormous number of immediately available facial images, pertaining to citizens who may never find themselves in situations that could lead to a criminal proceeding.

If law enforcement were provided with such a powerful and invasive tool, preventing abuses and limiting the app's use to what is strictly necessary may become a challenging undertaking for EU and national authorities. Arguably, the mere 'convenience' may not be enough to legitimize a generalized system of surveillance – like the one Clearview is planning to sell us – if we wish to preserve the restraints on power that are at the core of our democratic societies.

Acknowledgements

The author is grateful to Professor Carles Górriz López, Professor Michele Caianiello and Dr Giulia Lasagni for their comments on the first draft of the article, and to the two anonymous reviewers for their constructive feedback.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: This project was funded by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD 'Law, Science and Technology Rights of Internet of Everything' Grant Agreement No. 814177.