Clearview AI revelations spark action on use of facial recognition

Sam Jungyun Choi, **Hannah Lepow**, **Christopher Lin**, and **Ian Macdonald** of Covington & Burling LLP discuss legislative and regulatory developments following publication of news that searchable faceprints were being generated from billions of online images.

Since the *New York Times* article on Clearview AI (Clearview) in January 2020,[1] the company has come under scrutiny from legislators, regulators, and the public for its use of facial recognition technology (FRT). As a refresher—because January feels like years ago—the *New York Times* article described how Clearview sells access to a database of faceprints, developed from scraping billions of images from websites such as Google, Facebook, and Twitter and then using FRT to map the faces in those images to create searchable faceprints. Users can then upload photos to find matches; a service popular with law enforcement.

In the US, parties ranging from the ACLU to the Attorney General of Vermont have taken Clearview to court on various legal theories. In the legislative sphere, sparked by the protests against police misconduct in the United States, a new bill proposed in Congress would impose a moratorium on law enforcement's use of FRT. Similar rumblings can be seen across the Atlantic in the EU as well. EU data protection authorities have announced investigations into the company's compliance with the GDPR. In this article, we highlight new developments relating to FRT in the United States and in the EU as well as the legal challenges facing Clearview.

Scrutiny in the US Courts

Eight putative class actions were filed within days of publication of the Times article, and more have followed. The cases plead claims under a variety of state and federal laws, including:

- **Illinois Biometric Information Privacy Act** (BIPA). Seven of the putative class actions allege that Clearview violated BIPA, the Illinois statute that regulates the collection and use of biometric information. Plaintiffs Mutnick,[2] Hall,[3] Calderon,[4] Burke,[5] Broccolino,[6] McPherson,[7] and John[8] allege that Clearview's use of FRT on images of class members constitutes the capture of biometric identifiers under BIPA, and that Clearview did not obtain consent or meet the other requirements of the statute. The ACLU of Illinois has sued Clearview on similar grounds.[9] No court has yet issued a substantive opinion in these cases.
- **California Consumer Privacy Act** (CCPA). Burke, one of the plaintiffs who sued Clearview under BIPA, also asserted that Clearview violated the CCPA because it failed to give proper notice to consumers of its data collection before scraping their biometric data.[10] The CCPA's private right of action is very limited, and does not extend to the statute's notice requirements. Plaintiffs assert that California's Unfair Competition Law provides them with a private right of action with respect to the alleged CCPA violation.
- **State Consumer Protection Statutes**. Two private plaintiffs are seeking class certification in suits against Clearview with discrete claims under Californian and Virginian consumer protection statutes, and the Vermont Attorney General has brought a suit against the company under that state's consumer protection law. John, who also brought claims under BIPA, asserts that Clearview violated the California Business and Professional Code, alleging that Clearview's alleged theft and use of photographs constituted an unfair business practice.[11] A complaint in Virginia alleges that the company's use of FRT on class members'

UK ICO AND AUSTRALIA'S DPA TO INVESTIGATE CLEARVIEW AI INC

The UK's Data Protection Authority (the ICO) announced, on 9 July, that it will open a joint investigation with its Australian colleagues (the OAIC), into the personal information handling practices of Clearview AI Inc., focusing on the company's use of 'scraped' data and biometrics of individuals. It is reported that Clearview's system includes a database of more than three billion images that Clearview claims to have taken or "scraped" from various social media platforms and other websites.

Reflecting the fact that Elizabeth Denham is the Chair of the Global Privacy Assembly, the ICO is choosing to work with a non-European country on this Clearview investigation, as it did with Canadian DPAs on the Facebook/Cambridge Analytica investigation. However, both parties have left the door open to cooperate with other DPAs, as the issues are similar in every country. Accordingly, the ICO states "The OAIC and ICO will engage with other data protection authorities who have raised similar concerns, where relevant and appropriate." As Clearview has announced that it also provides its services to financial services companies and retailers, the focus in other countries could be on different sectors. The investigation highlights the importance of enforcement cooperation in protecting the personal information of Australian and UK citizens in a globalised data environment, the ICO says.

In Canada, the focus of the investigation by the Privacy Commissioners at national level and those in Alberta, British Columbia and Quebec is on the use by the Royal Canadian Mounted Police (RCMP) of Clearview services. Responding to these events, on 6 July, the company announced that, as a result of this investigation, it had stopped providing a service to the RCMP which anyway was its last client in Canada.

Stewart Dresner

• *See ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/*

photographs violated both the Virginia Computer Crimes Act and Virginia Code § 8.01-40, which the plaintiff asserts protect against the unauthorized use of name or picture of any person.[12] (The Virginia case is the only class action suit thus far not to also invoke BIPA.) The Vermont Attorney General is the only US regulator to bring an action against the company so far. The suit, in Vermont state court, alleges three claims under the state's consumer protection law: that Clearview's alleged use of FRT on screen-scraped photos of Vermonters constituted an unfair act and practice in commerce; that Clearview made false and misleading statements about its business in Vermont; and that Clearview brokered personal biometric information through fraudulent means.

- **Common Law Claims**. In addition to alleging violations of state statutes, plaintiffs in Mutnick, Burke, Broccolino, McPherson, and John also claim that Clearview is guilty of unjust enrichment to the extent that it allegedly profited from scraping of the class members' biometric markers and other data.
- **Federal Law Claims**. Only one case asserts federal claims. Plaintiff Mutnick, who also filed a claim under BIPA, claims that Clearview is a state actor by virtue of its selling its service to state agencies and police departments. Under this theory, Mutnick alleges four constitutional claims, under the First, Fourth, and Fourteenth Amendments as well as the Contracts Clause.[13] Mutnick alleges that: (i) Clearview conspired with state officials to deny class members' access to the courts in violation of the First Amendment; (ii) Clearview's alleged collation of biometric identifiers constituted an unlawful search and seizure under the Fourth Amendment; (iii) Clearview's alleged actions violated the Fourteenth Amendment's right to due process by exposing class members to various physical harms; and (iv) Clearview's alleged scraping of biometric data from public websites violated class members' contractual rights under the Contracts Clause.

In a court filing in May 2020, Clearview, seeking dismissal in the Mutnick case in Illinois federal court, stated that it was taking "comprehensive steps to prevent the collection of facial vectors from photos associated with Illinois, and to prohibit the searching of existing photos associated with Illinois."[14] In addition to ceasing operations in Illinois, Clearview announced that it was "terminating access rights to its app for all account holders based in Illinois and . . . the accounts of any non-law enforcement or government entity."[15]

Developments in FRT Legislation in the US

The US Congress has introduced two new legislative proposals seeking to regulate government use of FRT. On 25 June 2020, the House of Representatives passed the George Floyd Justice in Policing Act, which would ban the use of real-time FRT on body cameras worn by federal law enforcement officials, and would require a warrant for the use of FRT on such footage at a later time.[16] The bill would also prohibit state and local law enforcement from using certain grants for FRT-related expenses.

Second, and far more sweeping, the Facial Recognition and Biometric Technology Moratorium Act—introduced to Congress in late June 2020, in the House by Reps. Pramila Jayapal (D-WA) and Ayanna Pressley (D-MA) and in the Senate by Sens. Ed Markey (D-MA) and Jeff Merkley (D-OR)—would prohibit any federal agency or official from using any biometric surveillance system, or any information derived from a biometric surveillance system operated by another entity, subject to limited exceptions.[17] The bill would also prevent local police departments who employ FRT from receiving certain federal funds.

Sen. Markey also penned a public letter to the Department of Justice prior to announcing the bill.[18] According to the letter, the Drug Enforcement Agency; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Secret Service; and the Federal Bureau of Investigation are all using Clearview's product on a trial basis.

These two proposals follow a previously proposed bill prohibiting the use of FRT in public housing introduced by Sen. Booker in October 2019,[19] and a previous FRT moratorium bill introduced by Sens. Booker and Merkley (D-OR) in February 2020.[20]

Some localities have also advanced efforts to regulate FRT. In June 2020, the Boston City Council voted unanimously to ban the use of FRT by the city, following in the steps of San Francisco, Oakland, Cambridge, and other municipalities. Also in June 2020, the New York City Council voted to disclose the surveillance methods employed by the New York Police Department, which include FRT.

Legal developments in the European Union

As was the case in the United States, Clearview faced heightened regulatory scrutiny in the EU following the *New York Times* article. A number of data protection authorities, including in Sweden and Germany, launched investigations of Clearview's practices. In March 2020, Sweden's data protection authority began to investigate government use of Clearview technology and published plans to send inquiries to various departments, e.g., police, Coast Guard, etc., to determine (1) whether they used the technology and (2) whether the use was justified under an appropriate legal basis.[21] Similarly, in March 2020, the Hamburg data protection authority requested from Clearview information regarding its business model, sources of data, and scope of processing.[22] The Hamburg data protection commissioner has since separately noted that while use of Clearview may not be fundamentally problematic, storage of facial images requested by police on the servers of a private provider is likely to contravene national laws.[23]

In June 2020, the European Data Protection Board (EDPB), the independent European body that is mandated by the GDPR to facilitate the consistent application of data protection laws throughout the EU, specifically weighed in on Clearview. The EDPB released a statement noting, in relevant part, that it "has doubts as to

whether any Union or Member State law provides a legal basis for using a service such as offered by Clearview AI. Therefore, as it stands and without prejudice to any future or pending investigation, the lawfulness of such use by EU law enforcement authorities cannot be ascertained."[24] The EDPB further referred to its guidelines on the processing of personal data through video devices, which addresses the GDPR considerations when deploying FRT, and announced plans to undertake further work on the use of FRT by law enforcement authorities.

Conclusion

FRT was already the subject of legislative interest before the *New York Times* article on Clearview AI, but since then the topic has only gained more attention, among the public at large as well as legislators and regulators. As public opinion moves and the litigations, bills, and other actions mentioned in this article more forward, it remains important for those in the privacy space to track key developments in FRT and take a proactive stance in adapting to changes in policy and legislation.

AUTHORS

Sam Jungyun Choi and Hannah Lepow are Associates, Christopher Lin is a Legal Intern, and Ian Macdonald is a Summer Associate at Covington & Burling LLP.
Emails: jchoi@cov.com
hlepow@cov.com
imacdonald@cov.com

REFERENCES

1 Kashmir Hill, The Secret Company that Might End Privacy as We Know It, *N.Y. Times*, Jan. 18, 2020, www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
2 Complaint, Mutnick v. Clearview AI, Inc., 1:20-cv-512-SC (N.D. Ill. Jan. 20, 2020) (No. 1).
3 Complaint, Hall v. Clearview AI, Inc., No. 20-846 (N.D. Ill. Feb. 5, 2020) (No. 1).
4 Complaint, Calderon v. Clearview AI, Inc., 1:20-cv-1296-CM (S.D.N.Y. Feb. 13, 2020).
5 Complaint, Burke v. Clearview AI, Inc., 1:20-cv-3104-CM (S.D. Cal. Feb. 27, 2020).
6 Complaint, Broccolino v. Clearview AI, Inc., 1:20-cv-2222-CM (S.D.N.Y. Mar. 12, 2020).
7 Complaint, McPherson v. Clearview AI, Inc., 1:20-cv-3053-CM (S.D.N.Y. Apr. 15, 2020).
8 Complaint, John v. Clearview AI, Inc., No. 1:20-cv-3481-CM (S.D.N.Y. May 4, 2020).
9 Complaint, A.C.L.U. v. Clearview AI, Inc. (N.D. Ill. May 28, 2020), available at: https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint
10 Complaint, Burke v. Clearview AI, Inc., 1:20-cv-3104-CM (S.D. Cal. Feb. 27, 2020).
11 Complaint, John v. Clearview AI, Inc., No. 1:20-cv-3481-CM (S.D.N.Y. May 4, 2020).
12 Complaint, Roberson v. Clearview AI, Inc., No. 20-cv-111-RDA-MSN (ED. Va. Feb. 3, 2020) (Nos. 12-14).
13 Complaint, Mutnick v. Clearview AI, Inc., 1:20-cv-512-SC (N.D. Ill. Jan. 20, 2020) (No. 1).
14 Defendants' Memorandum of Law in Opposition to Plaintiff's Motion for Preliminary Injunction, Mutnick v. Clearview AI, Inc., 1:20-cv-512-SC, at 1 (N.D. Ill. May 26, 2020) (No. 1).
15 Defendants' Memorandum of Law in Opposition to Plaintiff's Motion for Preliminary Injunction, Mutnick v. Clearview AI, Inc., 1:20-cv-512-SC, at 1 (N.D. Ill. May 26, 2020) (No. 1).
16 H.R. 7120, 116th Cong. (2020), available at: www.congress.gov/bill/116th-congress/house-bill/7120
17 S. ___, 116th Cong. (2020), at: www.markey.senate.gov/imo/media/doc/acial%20Recognition%20and%20Biometric%20Technology%20Moratorium%20Act.pdf
18 www.markey.senate.gov/imo/media/doc/DOJ%20Protest%20Surveillance.pdf
19 No Biometric Barriers to Housing Act of 2019, S. 2689, 116th Cong. (2020), available at: www.congress.gov/bill/116th-congress/senate-bill/2689?overview=closed
20 Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020), available at: www.congress.gov/116/bills/s3284/BILLS-116s3284is.pdf
21 Swedish DPA Launches Investigation Into Use of Clearview AI, IAPP, Mar. 6, 2020, iapp.org/news/a/swedish-dpa-launches-investigation-into-use-of-clearview-ai
22 Hamburg's Datenschützer leitet Prüfverfahren gegen Clearview ein, Spiegel Netzwelt, Mar. 25, 2020, www.spiegel.de/netzwelt/web/clearview-hamburgs-datenschuetzer-leitet-pruefverfahren-ein-a-0ec1870d-c2a5-4ea1-807b-ac5c385ae165
23 Matthias Monroy, Clearview AI: What does Interpol Use Face Recognition For?, Mar. 9, 2020, digit.site36.net/2020/03/09/clearview-ai-what-does-interpol-use-face-recognition-for
24 edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf

EU to deploy 'controversial' traveller screening

Statewatch has released a report, Automated suspicion: The EU's new travel surveillance initiatives, according to which travellers' privacy will be infringed by the use of surveillance technologies. The report examines how all applicants for short-stay Schengen visas and new "travel authorisations" will be checked against millions of files in police databases, screened by automated profiling tools, and have their names checked against a new "pre-crime" watchlist operated by Europol.

"Before visitors arrive in the Schengen area, during their stay and after they leave, their data will be held in enormous centralised databases accessible by thousands of officials, and made available for a variety of uses such as identity checks and law enforcement investigations," Statewatch says.

Statewatch reports that the new profiling tools will try to detect potentially "risky" individuals who are unknown to the authorities through the use of "screening rules" and "risk indicators" relating to factors such as age range, nationality, country and city of residence, destination, purpose of travel and occupation. The new systems that underpin these changes are meant to be in place by the end of 2022, as part of the EU's plans to make policing and migration databases "interoperable", the report says.

• *See statewatch.org/automatedsuspicion*

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU-US Privacy Shield is invalid says European Court of Justice

Although Standard Contractual Clauses remain valid, the decision creates uncertainty for companies which have been relying on the Shield for their EU-US transfers. By **Laura Linkomies**.

The EU-US Privacy Shield was declared invalid by the Court of Justice of the European Union (CJEU) on 16 July. The court said that the agreement does not provide equivalence of protection to EU citizens due to access to personal data by the US surveillance community, and that there are faults in the US Ombudsman system. The US Department of Commerce, which administers the programme, was

Continued on p.3

Jamaica adopts a post-GDPR data privacy law

Graham Greenleaf asks whether Jamaica's law is strong enough to mark the start of a different direction for data privacy in the Caribbean.

Jamaica's Data Protection Act 2020[1], enacted on 19 May but not yet in force, provides for a transitional period of two years. The Jamaican Information Commissioner, once appointed, should be influential in the region, at least within the anglophone Caribbean.

There are now 15 Caribbean data privacy laws: the Bahamas (2003), St Vincent & Grenadines (2003), BES Islands (the Netherlands municipalities

Continued on p.5

Issue 166 **AUGUST 2020**

INTERNATIONAL report

ISSUE NO 166 **AUGUST 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Katharina Weimer
Fieldfisher, Germany
Phil Lee
Fieldfisher, UK
Sam Jungyun Choi, Hannah Lepow, Christopher Lin and Ian Macdonald
Covington & Burling LLP, US
Elizabeth Coombs
UN programme on the Right to Privacy
Sanna Toropainen
Muna.io, Belgium
Nerushka Bowan
The LITT Institute, South Africa
Professor Nohyoung Park
University of Korea

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Guidance needed from the European Data Protection Board

The decision from the Court of Justice of the European Union (CJEU) on the adequacy failings of the protection provided by the EU-US Privacy Shield has left organisations in confusion. While the Shield is out and Standard Contractual Clauses remain, organisations will have to satisfy themselves about the level of the data protection law in the country where they transfer data. National EU DPAs need to unite now in terms of their response (p.1).

Clearview's practices processing facial recognition data have been attracting the attention of individual DPAs, and collectively as the European Data Protection Board (EDPB). The EDPB is doubtful whether a legal basis can be found for using Clearview AI services in the EU (p.16).

As Amazon issues a one-year moratorium for police use of its facial recognition tech, the EU Commission ponders whether legislation is needed for AI (p.9). It is not expected that the GDPR will be amended in light of new technologies now that the Commission has made its and stakeholders' views clear in its review (p.24).

Last year, the Planet-49 case on cookies made organisations aware of the tricky issue of cookie consent. What has happened in Germany with this ruling of the CJEU, and how does it impact cookie compliance? Read our correspondent's analysis on p.10.

After a long wait, many parts of South Africa's privacy law are now in force (p.22), and Jamaica has legislated, mostly in GDPR-style (p.1). Both laws have GDPR-influenced definitions of common terms.

As the pandemic has put a strain on everyone's personal and professional life, what lessons can be learned on managing the crisis? Our contributor from Korea says that while his country is regarded as a successful in containing the spread of Covid-19, its actions have been criticised by privacy activists (p.26). Please send me (laura@privacylaws.com) your views on returning to the workplace after the pandemic (p.26).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*Privacy Laws & Business* helps me keep pace with the latest discussions on the topical issues in data protection. A critical resource at a time when there is continuous development in our understanding of the law as well as a shift in how businesses are using data."

Rachael Annear, Senior Associate, Freshfields Bruckhaus Deringer LLP

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.