Facing facts: The state of US and EU facial recognition legislation

By **Sam Choi**, **Hannah Lepow**, **Christopher Lin**, and **Jadzia Pierce** of Covington & Burling LLP.

Facial recognition technology (FRT) is being developed and deployed at phenomenal speeds and lawmakers worldwide are scrambling to catch up. The resulting pieces of legislative and enforcement efforts convey that although there is consensus that something needs to be done to regulate the burgeoning technology, there is little consensus on the approach that should be taken. In this article, we highlight some of the key trends that have come out of the United States and the European Union thus far.

United States

In the United States, legislative proposals can be divided into those seeking to regulate government use of FRT and those seeking to regulate commercial use of FRT.

Government use of FRT: Proposals aimed at regulating government use of FRT run the gamut from imposing complete moratoriums on such use to creating specific requirements and guidelines that agencies would be required to follow.

In February 2020, Sens. Jeff Merkley (D-OR) and Cory Booker (D-NJ) introduced the Ethical Use of Facial Recognition Act, which would prohibit any federal agency official from using FRT without a warrant until Congress enacts legislation implementing guidelines for such use.[1] As another example, in November 2019, Sens. Chris Coons (D-DE) and Mike Lee (R-UT) introduced the Facial Recognition Technology Warrant Act of 2019, which would prohibit using FRT for ongoing surveillance in a public space unless such surveillance is in support of a law enforcement activity and certain other conditions are met.[2]

State legislatures, meanwhile, have moved past legislative proposals and actually enacted legislation. In October 2019, California enacted A.B. 1215, which creates a three-year moratorium on law enforcement agencies' use of any biometric surveillance system in connection with police-worn body-cams.[3]

In March 2020, Washington state enacted a bill that prescribes several requirements for agency use of FRT.[4] Among other things, prior to deploying the technology, agencies will be required to file a notice of intent and publish an accountability report that will be subject to public review and comment. Use of FRT to make decisions that produce legal or "similarly significant" effects (e.g., decisions pertaining to financial services, housing, criminal justice, or employment opportunities) will be subject to heightened requirements. In addition, certain uses will be substantially limited, including the use of FRT for ongoing surveillance, real-time or near-real-time identification, or persistent tracking without a warrant (or in other limited circumstances).

Various states are considering their own pieces of legislation that regulate government use of FRT in a variety of ways, such as Arizona,[5] Massachusetts,[6] New Hampshire,[7] and Vermont.[8] In addition, multiple city governments have taken matters into their own hands — the cities of San Francisco,[9] Oakland,[10] and Somerville,[11] for example, have ordinances in place that largely ban city officials' use of FRT for surveillance.

Commercial use of FRT: Federal and state proposals aimed at regulating commercial use of FRT range from cross-sector regulation to bills that focus on a particular contexts, such as housing or employment.

The majority of the federal proposals addressing commercial use of FRT from this Congressional session are limited to spheres in which the federal government has some authority, such as through funding. For example, the No Biometric Barriers to Housing Act—introduced in the House by Representatives, Yvette Clarke (D-NY) in July 2019 and introduced in the Senate by Sen. Booker (D-NJ) in October 2019—would regulate the use of FRT by landlords who receive some form of federal financial assistance.[12] Similarly, a House bill proposed by Rep. Rashida Tlaib (D-MI) would prohibit any federal funding from being used for the purchase or use of FRT.[13]

We are aware of one federal proposal that would broadly regulate commercial use of FRT, without a federal funding hook. The Commercial Facial Recognition Privacy Act, introduced just over a year ago in March 2019 by Sen. Roy Blunt (R-MO), would prohibit commercial entities from, among other things, collecting facial recognition data from end users without affirmative consent.[14] The bill has not progressed since its initial referral to committee.

There are active bills seeking to regulate commercial use of FRT in nearly a dozen states, from California[15] and New Jersey[16] to Idaho[17] and Alabama.[18] The majority of these follow the formula of the broadest federal proposal, prohibiting the use of FRT without some type of notice provided to and/or consent obtained from the consumer. However, certain of the bills focus on specific issues. For example, the Maryland state legislature recently passed a bill prohibiting the use of FRT during job interviews without the applicant's consent.[19] Additionally, one New York proposal would prohibit landlords from using FRT in residential properties.[20] While none of the federal proposals discussed above include an express private right of action, several state bills do.[21]

European Union

In the EU, the General Data Protection Regulation (GDPR), and its law enforcement counterpart, the Police and Criminal Justice Directive, apply to commercial and government use of

FRT. Facial images are deemed personal data under the GDPR, meaning that controllers of FRT systems must comply with certain obligations — including transparency, processing data fairly and securely, and complying with individuals' requests to exercise rights they have over their personal data. Where facial images are used for the purpose of uniquely identifying individuals they constitute "special category personal data," and are subject to heightened obligations under the GDPR (Art. 9). In those circumstances, the controller may need to obtain explicit consent from individuals whose faces are processed by the FRT system, or alternatively, identify a substantial public interest for the processing under EU or Member State law.

In the last few years, FRT systems have been deployed in a range of different settings in Europe. Accordingly, a number of data protection authorities (DPAs) in different Member States have examined FRT use within the construct of the GDPR.[22] Notably, the European Data Protection Board, made up of representatives from DPAs in each Member State and formally established to issue GDPR guidance, has issued guidance on FRT use.[23] In some cases, DPAs have found that certain uses of FRT systems are in breach of the GDPR. For example, on 21 August 2019, Sweden's DPA fined the Skellefteå municipality for using FRT to track student attendance in a public school, concluding that: (1) tracking attendance with FRT was overly invasive, (2) the imbalance of power between the students (the data subjects) and the school (the data controller) invalidated student consent, and (3) the school did not conduct a data protection impact assessment.[24] In other cases, DPAs have permitted FRT use. For instance, the Danish DPA approved in July 2019 Brøndby Football Stadium's use of FRT to enforce a ban list for security purposes.[25] DPAs are continuing to investigate other uses of FRT, such as at London King's Cross development and by Clearview AI. [26]

In the UK, use of FRT systems was challenged from a human rights law perspective at the UK High Court.[27] The European Convention on Human Rights provides that everyone "has the right to respect for his private and family life, his home and his correspondence." (Art. 8.) With a few exceptions, public authorities may not interfere with the exercise of this right. The complainant alleged that South Wales Police Force's use of FRT for policing and security purposes infringed this fundamental human right, as well as UK data protection laws and equality legislation. The court found in favor of South Wales Police Force's use of FRT based on the specific facts of the case. Nonetheless, this case prompted the UK Information Commissioner to investigate and issue an opinion on police use of FRT, calling on the UK government to introduce a statutory binding code of practice on the use of biometric technology, such as live facial recognition technology.[28]

Further regulation of FRT, particularly by public authorities, remains an open issue in the EU. Although the GDPR offers safeguards for individuals whose facial images are processed by FRT systems, some policymakers and commentators think that these measures do not go far enough to protect fundamental human rights. This debate over the need for further FRT regulation has arisen at the EU level in the context of future regulation of AI technologies. On 19 February 2020, the European Commission published a White Paper on AI,[29] setting out the EU's vision for building an "ecosystem of trust" regarding AI use in the EU through a robust legislative framework. Among other things, the White Paper proposes a mandatory pre-marketing conformity assessment requirement for high-risk AI applications. The Commission recognizes "remote biometric identification systems" — such as FRT use in public spaces — as an example of a high-risk AI application that could be subject to this conformity assessment requirement. In the White paper, the Commission notes that FRT systems are already heavily regulated under existing EU laws (as described above), but that there are unique concerns raised by their deployment in public spaces. The Commission further states that it will "launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards."[30]

Conclusion

Although FRT has become a popular topic among lawmakers, it is unclear whether varying legislative and enforcement efforts may someday converge into a unified approach. What is clear is that lawmakers' activities nevertheless may influence the technology's continued development and use. As a result, it will be critical to continue to track key developments and be prepared to adapt, as needed.

AUTHORS

Sam Choi, Hannah Lepow and Jadzia Pierce are Associates, and Christopher Lin is a Legal Intern, at Covington & Burling LLP in the US.
Emails: jchoi@cov.com
hlepow@cov.com
jpierce@cov.com
clin@cov.com

REFERENCES

1 S. 3284, 116th Cong. (2020), available at www.congress.gov/116/bills/s3284/BILLS-116s3284is.pdf
2 S. 2878, 116th Cong. (2019), available at www.congress.gov/116/bills/s2878/BILLS-116s2878is.pdf
3 A.B. 1215, 2019–2020 Leg., Reg. Sess. (Cal. 2019), available at leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201920200AB1215&version=20190AB121593CHP
4 Alex Berengaut & Jadzia Pierce, InsidePrivacy.com, Washington State Passes Bill Limiting Government Use of Facial Recognition (Mar. 23, 2020), www.insideprivacy.com/united-states/state-legislatures/washington-state-passes-bill-limiting-government-use-of-facial-recognition/
5 S.B. 1383, 54th Leg., 2d Reg. Sess. (Ariz. 2020), available at www.azleg.gov/legtext/54leg/2R/bills/SB1383P.pdf
6 S. 1385, 91st Gen. Ct. (Mass. 2019), available at malegislature.gov/Bills/191/S1385.pdf
7 H.B. 1642, 2020 Leg. (N.H. 2020), available at

REFERENCES

gencourt.state.nh.us/bill_status/billText.aspx?id=1202&txtFormat=html&sy=2020

8 H. 923 (Vt. 2020), available at legislature.vermont.gov/bill/status/2020/H.929

9 City of San Francisco, Cal., Stop Secret Surveillance Ordinance, available at sfgov.legistar.com/LegislationDetail.aspx?ID=3850006&GUID=12FC5DF6-AAC9-4F4E-8553-8F0CD0EBD3F6

10 City of Oakland, Cal., Surveillance Equipment Ordinance Amendment, available at oakland.legistar.com/LegislationDetail.aspx?ID=3976661&GUID=CB1D4794-7549-485A-A345-B7B38B38E191

11 City of Somerville, Mass., Face Surveillance Full Ban Ordinance, available at somervillecityma.iqm2.com/Citizens/Detail_LegiFile.aspx?Frame=&MeetingID=2961&MediaPosition=&ID=20991&CssClass

12 H.R. 4008, 116th Cong. (2019), available at www.congress.gov/116/bills/hr4008/BILLS-116hr4008ih.pdf; S. 2689, 116th Cong. (2019), available at https://www.congress.gov/116/bills/s2689/BILLS-116s2689is.pdf

13 H.R. 3875, 116th Cong. (2019), available at www.congress.gov/116/bills/hr3875/BILLS-116hr3875ih.pdf

14 S. 847, 116th Cong. (2019), available at www.congress.gov/116/bills/s847/BILLS-116s847is.pdf

15 A.B. 2261, 2019–2020 Leg., Reg. Sess. (Cal. 2020), available at leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB2261

16 A.B. 3625, 219th Leg. (N.J. 2020), available at www.njleg.state.nj.us/2020/Bills/A4000/3625_I1.PDF

17 H.B. 492, 65th Leg., 2d Reg. Sess. (Idaho 2020), available at legislature.idaho.gov/sessioninfo/2020/legislation/H0492/

18 H.B. 295, 2020 Leg., Reg. Sess. (Ala. 2020), available at legiscan.com/AL/text/HB295/id/2143609/Alabama-2020-HB295-Introduced.pdf

19 H.B. 1202, 2020 Leg., 441st Sess. (Md. 2020), available at mgaleg.maryland.gov/2020RS/bills/hb/hb1202T.pdf

20 S. 5687, 2019–2020 Leg., Reg. Sess. (N.Y. 2019), available at www.nysenate.gov/legislation/bills/2019/s5687

21 See West Virginia, H.B. 4106, 2020 Reg. Sess. (W.V. 2020), available at www.wvlegislature.gov/Bill_Text_HTML/2020_SESSIONS/RS/bills/HB4106%20INTR.pdf; Hawaii, S.B. 3148, 30th Leg. (Hawaii 2020), available at egiscan.com/HI/text/SB3148/id/2135163/Hawaii-2020-SB3148-Amended.html; Maryland, H.B. 307, 2020 Leg., 441st Sess. (Md. 2020), available at legiscan.com/MD/text/HB307/id/2171696/Maryland-2020-HB307-Engrossed.pdf; New York, S. 1203, 2019–2020 Leg., Reg. Sess. (N.Y. 2019), available at legislation.nysenate.gov/pdf/bills/2019/S1203

22 See, e.g., Kristof Van Quathem & Anna Oberschelp de Meneses, InsidePrivacy.com, French Supervisory Authority Publishes Guidance on Facial Recognition (Nov. 18, 2019), www.insideprivacy.com/data-privacy/french-supervisory-authority-publishes-guidance-on-facial-recognition

23 See European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices (Jan. 30, 2020), edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

24 European Data Protection Board, Facial Recognition in School Renders Sweden's First GDPR Fine (Aug. 22, 2019), edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en; Sofia Evardsen, International Association of Privacy Professionals, How to Interpret Sweden's First GDPR Fine on Facial Recognition in School (Aug. 27, 2019), iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school

25 European Digital Rights, Danish DPA Approves Automated Facial Recognition (June 19, 2019), https://edri.org/danish-dpa-approves-automated-facial-recognition.

26 Meera Narendra, Data Protection World Forum, #Privacy: Swedish DPA Announces Investigation Into the Use of Clearview AI (Mar. 9, 2020), gdpr.report/news/2020/03/09/privacy-swedish-dpa-announces-investigation-into-the-use-of-clearview-ai; Information Commissioner's Office, Statement: Live Facial Recognition Technology in King's Cross (Aug. 15, 2019), ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross.

27 *R. (Bridges) v. Chief Constable of South Wales Police*, [2019] WLR (D) 496 (U.K.).

28 Sam Jungyun Choi, UK's Information Commissioner Issues Opinion on Use of Live Facial Recognition Technology by Police Forces (Nov. 5, 2019), www.insideprivacy.com/data-privacy/ai-iot-update-uks-information-commissioner-issues-opinion-on-use-of-live-facial-recognition-technology-by-police-forces/

29 European Commission, White Paper: Artificial Intelligence - A European approach to excellence and trust (Feb. 19, 2020), COM(2020) 65 final, ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

30 *Id*. at 22.

Joint investigation into Clearview's use of facial recognition

The Privacy Commissioner of Canada and the Privacy Commissioners in the provinces of Quebec, British Columbia and Alberta have announced that they will jointly investigate Clearview AI and its use of facial recognition technology.

The investigation was initiated in the wake of numerous media reports that have raised questions and concerns about whether the company is collecting and using personal information without consent. "Media reports have stated that Clearview AI is using its technology to collect images and make facial recognition available to law enforcement for the purposes of identifying individuals," the DPAs say.

"Privacy regulators in every province and territory have also agreed to work together to develop guidance for organizations – including law enforcement – on the use of biometric technology, including facial recognition."

• *See www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/*

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Indonesia's DP Bill lacks a DPA, despite GDPR similarities

Graham Greenleaf and **Andin Aditya Rahman** of Assegaf Hamzah & Partners, Indonesia, analyse the Bill's provisions.

Indonesia's long-awaited comprehensive draft Law on the Protection of Personal Data ("the Bill") has been submitted by President Joko Widodo to the Chairperson of the Indonesian House of Representatives. Minister of Communication and Information, Johnny G. Plate announced the submission on 28 January 2020 and was summoned by the House to elaborate on the Bill in a formal meeting at the end of February, after which he stated that he expected the Bill will

Continued on p.3

Finland invests in European cooperation, prepares to fine

Finland's DPA's workload has stabilised after the immediate post-GDPR rush. The first GDPR fines are now in the pipeline. **Laura Linkomies** reports from Helsinki.

As Finland prepares to issue its first administrative fines under the GDPR, most likely by the beginning of May, the Data Protection Ombudsman, Reijo Aarnio, says that it is of paramount importance to achieve consistency across EU member states regarding the size of fines.

There was some delay in setting up the administrative structure to enable the issuing of fines. Anu Talus,

Continued on p.7

Covid-19 delays PL&B Events

- *Nowhere to Hide*, PL&B's 33rd Annual International Conference, will transfer from Cambridge to London and from summer to autumn. Please see www.privacylaws.com/ac for a speaker list and details of their sessions.
- We have also postponed *Germany's Data Protection Law: Trends, Opportunities & Conflicts*, to be hosted by Covington & Burling in London, from March, until the autumn. See www.privacylaws.com/germany

privacylaws.com

Issue 164 **APRIL 2020**

INTERNATIONAL report

ISSUE NO 164 APRIL 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
Andin Aditya Rahman
Assegaf Hamzah & Partners, Indonesia
Nick Rhodes
BAE Systems Applied Intelligence, UK
Colin J. Bennett
University of Victoria, Canada
Tripti Dhar
Reina Legal LLP, India
Oliver Butler
Oxford University, UK
Tayebeh Saheb
Modares University, Iran
Elizabeth Coombs
UN SRP Taskforce
Sam Choi, Hannah Lepow, Christopher Lin, and Jadzia Pierce
Covington & Burling LLP, US

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

DPAs respond to Covid-19

We are all affected by the coronavirus pandemic, and not least in our private lives. Suddenly restrictions to civil liberties that would have seemed draconian feel acceptable if suitable safeguards are provided, for example, using mobile phone data to monitor the spread of the virus (p.15) by means of tracking our movements. It is pleasing that the global DPA community has concluded that data protection law does not stop data sharing for Covid-19 purposes (p.25) – but at the same time we need to stay vigilant that the current exceptions do not become the norm in future. DPAs have issued statements and guidance on the coronavirus situation for organisations whose privacy compliance teams are now often working remotely. Much of that is related to the kind of data which can be gathered on employees, but there is also guidance on how to manage data security issues for remote workers. In addition, the European Union Agency for Cybersecurity (ENISA) on 24 March issued its top tips for cybersecurity when working remotely.

For everyone who has suddenly needed to take up new technologies to organise virtual meetings, Zoom has become a popular option. However there have been reports of Zoom's bad track record with data protection measures. Zoom has defended itself by saying that "No data regarding user activity on the Zoom platform – including video, audio, and chat content – is ever provided to third parties for advertising purposes." In the US, a class action lawsuit has been launched, and on 1 April the Hong Kong Privacy Commissioner for Personal Data made data security recommendations to Zoom users.

Before the travel restrictions kicked in, I was in Finland to interview the Ombudsman and his Deputy (p.1), and a travel app company Whim (p.28). Other articles in this issue include a world first analysis (in English) of Indonesia's new data protection Bill (p.1), updates on Canada (p.16), Iran (p.26), Dubai (p.13), data ethics (p.10), facial recognition (p.22), and privacy aspects of gender equality (p.30). In this issue, we also report on digital identity developments in Africa and the Middle East (p.18).

Unfortunately, we have had to move *Nowhere to Hide*, PL&B's 33rd Annual International Conference from Cambridge to London and from summer to autumn. Please see our website at www.privacylaws.com/ac for a speaker list and details of their sessions. Most speakers will be, in principle, available for our conference, which we can arrange only when social distancing stops and travel starts.

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

"I would like to congratulate the editors of *Privacy Laws & Business*. This Report gives me the latest information and useful suggestions that are a great help for my research projects. This magazine is very valuable for anyone involved in privacy."

Professor Fumio Shimpo, Department of Policy Management, Keio University, Japan

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.