# Clearview AI exposes our regulatory shortcomings

**Marcin Betkier, Privacy Foundation New Zealand**
Opinions expressed do not express the official view of the Foundation

The case of Clearview AI and its facial recognition app which is widely commented on in the media[1] perfectly exposes the problems of the current New Zealand privacy law. Clearview scrapes photos and videos from Facebook, YouTube and other publicly available websites to create a gigantic database of 3 billion photos of faces. Then, their smartphone app can be used to match the face with a photo taken, for example, on the street, with the photos in that database and reveal the information about the person. This software is currently sold only to law enforcement agencies. But, the method of collecting such a database by scraping publicly available services has been revealed and anyone can do the same. That is, make possible to show our 'digital dossier' to anyone on the street.

New Zealand's Privacy Act 1993 offers individuals no help to that problem. That is, Information Privacy Principle 2 allows Clearview or alike to collect indirectly the personal information that is already publicly available. And, there is no obligation to inform an individual about such indirect collection. Of course, Clearview may breach the Terms & Conditions of other services which may take legal action. But we do not know whether our photos were scraped. And, even if we knew about it, there are no legal tools to object to processing of that data or request erasure. So, we do not know about our data collection and even if we knew we could do little about it.[2]

Could the Privacy Bill, the long-awaited overhaul of our Privacy Act 1993, help us with that? The Bill is still in the Committee of the whole House and the House, to put it mildly, seems to be not the same fastest legislature in the west as it happened to be. But, even if the Bill is enacted this year, it still gives no tools to deal with Clearview and the like. Compliance notices, a new Privacy Commissioner's tool, requires breach of a privacy principle to trigger such action.

So, if the Privacy Act 1993 and Privacy Bill are chasing the past, what could we do? We could simply look around for the necessary tools. The Office of the Canadian Privacy Commissioner has begun an investigation against Clearview pointing out that the company is collecting personal data without users' consent.[3] The European GDPR provides for both, the information about the indirect collection (Article 14) and for 'removal tools' – withdrawing consent, the rights to object and to erase the data (Articles 7, 17, 21). Both, the Canadian 'soft consent' and the presented GDPR mechanisms could possibly address the challenge of problems such as this. We need it now.

But, the discussion we should really be having now is about the future. Artificial Intelligence, facial recognition technologies, threats to democracy, strategies that speed up the

---

[1] "The trouble with Clearview AI, how your website watches you" (20 February 2020) RNZ <www.rnz.co.nz>; Kashmir Hill "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (18 January 2020) <www.nytimes.com>.

[2] It should be noted that potentially Information Privacy Principle 4 could be engaged if we classify such scraping as unfair. This, however, is not clear on these facts.

[3] Office of the Privacy Commissioner of Canada "Announcement: Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology" (21 February 2020) <www.priv.gc.ca>.

development of data economy – these are the topics for discussion in the US and in Europe. We need a data strategy that embraces strong privacy safeguards for individuals. That could protect individuals and, at the same time, oil the wheels of markets that do not want risks associated with privacy (and need 'adequacy' with the global laws to facilitate data flows).

For example, the European Union just published 'A European strategy for data' and 'White Paper on Artificial Intelligence'.[4] They recognise the importance of privacy and data protection for creating trust and safe 'data spaces' that could boost economic growth. Even in the United States, traditionally reluctant to regulate their data economy, California has just implemented the California Consumer Privacy Act (CCPA), a lighter version of the GDPR. Also, a number of federal level privacy bills are currently being discussed in the US Congress.

And here in NZ? We are waiting for the new law that is obsolete even before enacting and each following month of waiting makes the gap even bigger... It seems that the only hope for us is that those unwilling 'donors' of our photos, such as Facebook and others, will fight for our data. But, it would be naïve to count on them. Do we have any politicians that are capable to see the challenges of the future?

[4] European Commission *A European strategy for data* (COM(2020) 66 final 2020); European Commission *White Paper On Artificial Intelligence* (COM(2020) 65 final 2020).