Robson Crim Legal Blog
Canada's Criminal Law Blawg

Clearview AI & Facial Recognition Technology: The End of Privacy?

By L Balagus

Last month, after multiple denials, the Ontario Provincial Police admitted to using Clearview AI facial recognition technology.[1] The Halifax Regional Police and members of the Edmonton Police Service also confirmed their officers had been using the software.[2] Later, the RCMP followed suit, confirming their use of the software and prompting the Office of the Privacy Commissioner to announce an investigation.[3]

While law enforcement have been using facial recognition technology for years, Clearview AI goes far beyond what was previously available. Its developers created an algorithm to scrape the entire internet for images, including Facebook and Youtube, to create a database of unprecedented size with over three billion images.[4] A user then uploads a photo or video still and in a matter of seconds the software will match it with all publicly available images, as well as links to where the images came from. Even images that have since been deleted, or from accounts that are now private, remain in Clearview's database.[5] In addition, Clearview's technology can identify faces from several different angles, unlike the facial recognition software typically used by law enforcement that requires the subject to be looking straight ahead, as in a mug shot or

[1] David Lao, *Clearview AI: When can companies use facial recognition data?* (March 2020), online: Global News <perma.cc/2FYC-ZFVC>.

[2] Emily Mertz, *Reviews launched after 3 Edmonton police officers use Clearview AI facial recognition software* (March 2020), online: Global News <perma.cc/6PGT-QYZ9>; Alexander Quon, *Halifax police confirm use of controversial Clearview AI recognition technology* (March 2020), online: Global News <perma.cc/EPN6-GL4B>.

[3] Andrew Russell, *RCMP used Clearview AI facial recognition tool in 15 child exploitation cases, helped rescue 2 kids* (March 2020), online: Global News <perma.cc/GZ8L-PRY2>.

[4] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It* (February 2020), online The New York Times <perma.cc/9UBY-4LML>.

[5] Donie O'Sullivan, *This man says he's stockpiling billions of our photos* (February 2020), online: CNN <perma.cc/G25G-FL33>.

passport id photo. Any image of the subject, even images where they are in the background, will be collected and gathered into a report to anyone who purchases Clearview AI.

Facial recognition technology like Clearview AI poses many risks to Canadian society. Essentially these risks can be divided into two main categories: risks when the technology works and risks when it doesn't.[6] When the technology is working, its pervasiveness means we do not always know when our image is being captured. Unlike other law enforcement identification tools, facial recognition does not give you a choice. I can choose not to give my DNA or fingerprints to the police, whereas I have no way to opt out against a facial recognition camera, aside from avoiding all public spaces. With Clearview AI's ability to identify your image even in profile, this software is potentially one of the most invasive threats to our privacy rights ever created.

Yet the risks associated with facial recognition technology when it doesn't work typically receive more attention. Technology and artificial intelligence are often prized for their ability to be objective and unbiased. If a police officer identified a suspect, and Clearview AI identified a subject, we would likely trust the conclusion of the software over the person. However, facial recognition is not always accurate, in particular for images of visible minorities.[7] These communities have historically been targets of racial profiling by police. With this new technology, higher rates of inaccurate matches will only serve to further exacerbate the discrimination these communities have endured.

[6] Lexi Michaud & Alicia Krausewitz, *The Eye in the Sky: Facial Recognition Technology and the New Surveillance State* (March 2020), online: McGill Law Journal Podcast <lawjournal.mcgill.ca/podcasts>.
[7] *Ibid.*

Section 8 of the *Canadian Charter of Rights and Freedoms* guarantees Canadians a reasonable expectation of privacy.[8] The jurisprudence in this area of the law has primarily developed by police using new technology to gather evidence and judges deciding whether it violated the expectations of privacy under section 8 or not.[9] Facial recognition technology presents a unique challenge to this pattern, as we have seen with the Toronto Police, for example, who denied using Clearview AI for months only to later reveal they had been using it. If police are not taking facial recognition evidence before a court, judges are not able to determine if its usage is constitutionally valid or not. Law enforcement needs to obtain warrants for technologies like GPS tracking, yet they are not for facial recognition technology, which is far more intrusive to our privacy rights.[10]

Some academics have pointed to *R v Spencer* as a potential avenue to further develop the use of facial recognition technology by law enforcement.[11] In *Spencer*, the court ruled collecting subscriber information from internet service providers was an infringement of section 8 rights against unreasonable search and seizure.[12] A critical insight we can take away from *Spencer* is the court's more nuanced view of technology. The court understood providing the name and address of an internet subscriber is not invasive in and of itself. Instead, it is how all internet activity is tied to that subscription, how the subscriber information is a gateway to all online activity, which is the core of privacy concerns.

[8] Richard Jochelson & David Ireland, *Privacy in Peril: Hunter v Southam and the Drift from Reasonable Search Protections* (Vancouver: UBC Press, 2019) at 26.

[9] See *R v Reeves*, 2018 SCC 46; *R v Jones*, 2017 SCC 60; *R v Tessling*, 2004 SCC 67.

[10] *Supra* note 6.

[11] *Ibid*.

[12] *R v Spencer*, 2014 SCC 43 at paras 32-33.

Similarly, our images and faces are not sensitive information, in that we are out and about in public with our faces visible all the time (or at least we were). Now, facial recognition technology can identify or link us to places and activities just like an ISP address links us to all our online activity. Future cases under Section 8 which follow *Spencer* could perhaps address to what extent a reasonable expectation of privacy includes some form of anonymity in public spaces against technology like Clearview AI.

As with any new technology, facial recognition software can be both a curse and a blessing to society. For instance, RCMP were able to use Clearview AI as part of investigations into online child sexual exploitation, resulting in the rescue of two children. It is easy to see how the advantages gained in finding guilty people could outweigh its risks to privacy. Nonetheless, more information and study is undoubtedly needed to determine the effectiveness of this technology. Its accuracy, or lack thereof, needs to be better understood to determine to what extent the technology actually improves the abilities of law enforcement. We also must consider the impact of a 'chilling effect' on the freedom of Canadians that could result from the widespread surveillance of our society.[13] Perhaps regulations could be developed to curb usage of this technology, allowing certain actors to employ this technology in specific circumstances, instead of an outright ban. Of course, like any other new technology, governments will be slow to act in developing these regulations. Overall, what Clearview AI demonstrates is that any benefit facial recognition technology offers must be carefully and considerately balanced with *Charter* rights and our reasonable expectation of privacy.

[13] *Ibid*.

TABLE OF AUTHORITIES

JURISPRUDENCE

R v Jones, 2017 SCC 60

R v Reeves, 2018 SCC 46

R v Spencer, 2014 SCC 43.

R v Tessling, 2004 SCC 67

SECONDARY MATERIALS

Hill, Kashmir, *The Secretive Company That Might End Privacy as We Know It* (February 2020), online The New York Times <perma.cc/9UBY-4LML>.

Jochelson, Richard & David Ireland, *Privacy in Peril: Hunter v Southam and the Drift from Reasonable Search Protections* (Vancouver: UBC Press, 2019).

Lao, David, *Clearview AI: When can companies use facial recognition data?* (March 2020), online: Global News <perma.cc/2FYC-ZFVC>.

Mertz, Emily, *Reviews launched after 3 Edmonton police officers use Clearview AI facial recognition software* (March 2020), online: Global News <perma.cc/6PGT-QYZ9>;

Michaud, Lexi & Alicia Krausewitz, *The Eye in the Sky: Facial Recognition Technology and the New Surveillance State* (March 2020), online: McGill Law Journal Podcast <lawjournal.mcgill.ca/podcasts>.

O'Sullivan, Donie, *This man says he's stockpiling billions of our photos* (February 2020), online: CNN <perma.cc/G25G-FL33>.

Quon, Alexander, *Halifax police confirm use of controversial Clearview AI recognition technology* (March 2020), online: Global News <perma.cc/EPN6-GL4B>.

Russell, Andrew, *RCMP used Clearview AI facial recognition tool in 15 child exploitation cases, helped rescue 2 kids* (March 2020), online: Global News <perma.cc/GZ8L-PRY2>.