RACIAL PROFILING IN THE INFORMATION AGE

J.M. Porup is a freelance national security and cybersecurity reporter based in Toronto. His work has appeared in the CBC, The Economist, Christian Science Monitor, Ars Technica, Vice Motherboard, and many others. Follow him on Twitter: @toholdaquill.

The internet disrupts democracy and turns Canada into a totalitarian dictatorship run by the secret police. This enables human rights violations on a massive scale. Computerized tools build racism into the heart of this new system. Predictive policing and sentencing algorithms automate racism. Government hacking and mass surveillance destroy democracy and concentrate power in the hands of Canada's state-sponsored terrorists — CSIS, CSE, and the covert branch of the RCMP.

Racial profiling is not hard to identify in meatspace. When police engage in carding or suspicionless stop-and-frisk in the street, for example, we as a society can perceive racial profiling at work. Awareness of the problem makes a public conversation possible, and puts solutions within reach.

But what about on the internet? We used to say we lived "in the real world" and went online. But in a very real sense, we now live online. Even if we never touch a computer, our world is built on computers. And the rules are different here. Power in the cyber domain changes the equation, and makes possible new forms of racial profiling that are far less obvious.

The Ontario Human Rights Commission (OHRC) currently defines racial profiling as

> "**any action** undertaken for **reasons of safety, security or public protection** that relies on **stereotypes** about race, colour, ethnicity, ancestry, religion, or place of origin rather than on reasonable suspicion, to single out an individual for greater scrutiny or different treatment." The OHRC adds that "profiling can occur because of a combination of the above factors and that age and/or gender can influence the experience of profiling."[1]

This paper will examine the ways in which racial profiling may ultimately reproduce itself in the cyber domain through the following mechanisms: *1)* predictive policing, *2)* sentencing algorithms, *3)* targeted hacking tools, and *4)* mass surveillance.

PREDICTIVE POLICING

Predictive policing is an attempt to prevent crime by predicting where crime will happen next. Algorithms analyze large quantities of data to identify crime hot spots, rate citizens with a "heat score" that indicates their likelihood of committing a crime, and help deploy police resources more efficiently.[2]

But for these algorithms to work, they must be implemented impartially (that is, without a built-in racial profiling bias), and they must be trained on impartial data.

1 Ontario Human Rights Commission Inquiry Report, Paying the Price: The Human Cost of Racial Profiling (21 October 2003) at 6. Also available online: http://www.ohrc.on.ca/en/paying-price-human-cost-racial-profiling/what-racial-profiling. Emphasis in the original.

2 http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist

On both counts predictive policing fails.

As Ronald Bailey wrote for *Reason*, "The accuracy of predictive policing programs depends on the accuracy of the information they are fed."[3]

The ACLU of Massachussetts explains, "If an algorithm is only fed unjust arrest data, it will simply repeat the injustice by advising the police to send yet more officers to patrol the black area. In that way, predictive policing creates a feedback loop of injustice."[4]

In other words, if past policing data skews heavily towards policing certain neighborhoods for certain types of offenses, then the predictive policing algorithm will do no more than "predict the past."

Further, these algorithms are designed by private companies and their methodology is opaque to the public being policed. How does the algorithm work? Is there built-in bias — either conscious, or unconscious?

Shouldn't this kind of "pre-crime" policing be accompanied by full and open disclosure about how the system works?

If that weren't enough to seriously question the wisdom of predictive policing, an investigation by the *San Francisco Weekly* concluded that there is no public evidence that predictive policing is effective, writing, "The future of policing looks a lot like good branding."[5]

The *Toronto Star* reports that predictive policing is already being deployed in Canada.[6] This does not bode well for Ontario and other provinces where information on "street-checks" or carding reveal that African Canadians and other racialized people already receive a disproportionate amount of attention from police services.

SENTENCING ALGORITHMS

When judges hand down sentences in criminal courts across the United States, in many cases courts are now using a sentencing algorithm that rates each convict on the likelihood of recidivism.

However, an investigation by ProPublica found that the sentencing algorithm was biased against black convicts.[7]

Even the former US attorney general had concerns about the use of sentencing algorithms. ProPublica reports that in 2014 Eric Holder "warned that the risk scores might be injecting bias into the courts. He called for the U.S. Sentencing Commission to study their use. 'Although these measures were crafted with the best of intentions, I am concerned that they inadvertently undermine our efforts to ensure individualized and equal justice," he said, adding, "they may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice system and in our society.'"[8]

The ProPublica investigation concluded that:

In forecasting who would re-offend, the algorithm made mistakes with black and white defendants at roughly the same rate but in very different ways.

- The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants.

- White defendants were mislabeled as low risk more often than black defendants.

Machine learning is automated bureaucracy. Bureaucrats bring their personal biases and prejudices to their work, often unconsciously. The programmers who designed and build these kinds of algorithms do too.

Decisions that deprive citizens of their liberty are not improved by automating prejudice and then hiding behind the mysterious workings of an opaque computer program.

Are sentencing algorithms employed in sentencing convicts in Canadian courts? If they are, is it even possible to avoid the role that racial profiling plays within this kind of system?

TARGETED HACKING TOOLS

Suspicionless searches by police based on race, creed, or country of origin violate Ontario's *Human Rights Code* (Code) — both online and off.

Police departments around the world now routinely hack into suspects' smartphones, laptops, tablets, even internet-connected home devices, like an Amazon Echo, in order to listen in using

3 https://reason.com/archives/2012/07/10/predictive-policing-criminals-crime

4 https://privacysos.org/predictive

5 http://www.sfweekly.com/sanfrancisco/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/Content?oid=2827968

6 https://www.thestar.com/news/gta/2016/05/10/surveillance-and-predictive-policing-welcome-to-the-safety-state-of-tomorrow.html

7 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

8 *Ibid.*

the device microphones, or watch using the device camera.[9] In June, 2016, a US appeals court ruled that police do not need a warrant to hack into a suspect's device.[10]

Suspicionless hacking "stop-and-frisk" of our smartphones and other devices is becoming a norm around the world. Such suspicionless searches disproportionately affect racialized groups, since, in this new world, smartphone security has become a luxury good that leaves the poor vulnerable to criminals and police abuse. Case in point, while Apple's iPhone has been widely recognized as one of the most secure computing devices that money can buy, Google's Android operating system, by contrast, although generally more affordable, is widely condemned for its poor security. This puts users at risk not only of financially-motivated malware, but makes it easy for police to hack into their phones. Android's poor security posture leaves the door open for racial profiling by police engaged in warrantless hacking of cell phones.

If not in use already, it appears that Canadian police forces are very interested in acquiring hacking tools. What rules then ultimately govern its use by police forces, such as the Toronto Police Services?[11] What prevents police services across all jurisdictions from hacking internet-connected devices based on racial profiling?

MASS SURVEILLANCE

In 2013, leaks about the National Security Agency (NSA) in the U.S. by whistleblower and former Central Intelligence Agency employee Edward Snowden revealed that mass surveillance is an extensive and prominent feature not only of America's security apparatus, but also of Canada's. Specifically, private communications by virtually all citizens are being collected, stored, and analyzed without their knowledge or authorization.

The NSA pools this data with communications collected by the other members of the Five Eyes (FVEYES) spying alliance, which includes the spying agencies of the US, UK, Canada, Australia, and New Zealand.

Analyzing the vast amount of data collected requires these spying agencies to use algorithms to automate the process. As I have previously reported, the NSA used a machine learning algorithm to rate each citizen on their likelihood of engaging in terrorist activity.[12] An entire country's cell phone traffic was analyzed to rate people on their "terroristiness." This NSA SKYNET algorithm turned out to be flawed and mislabeled thousands of innocent Pakistanis as terrorists, who may have been droned to death as a result.

Although such revelations have not been divulged with respect to any security agency in Canada, it is not beyond the realm of possibility that a similar machine learning algorithm could be used to score Canadian citizens and residents on their likelihood of committing a terrorist or criminal act. This would certainly open the door to validating the kinds of racial profiling that are all too pervasive in our society.

CONCLUSION

The struggle to defend human rights has moved online. In many ways, information technology enables human rights violations on a global scale. Hacking tools and mass surveillance used by spy agencies and police services subvert the rule of law and violate our human rights. The use of predictive policing and sentencing algorithms are increasingly being viewed as acceptable, despite clear examples of the role that racial profiling play in its function.

Defending human rights, as embodied by the *Code*, requires us to examine abuses not just "in the real world," but also online.

9 https://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech

10 https://www.eff.org/deeplinks/2016/06/federal-court-fourth-amendment-does-not-protect-your-home-computer

11 https://news.vice.com/article/canadian-police-spies-eyed-hacking-team-tech-and-the-law-now-makes-it-easier-to-acquire

12 http://arstechnica.co.uk/security/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people