Yuwen Zhang

Gleneagle Secondary School

Grade 12

1389 words

RULE OF LAW: UNDER SURVEILLANCE

"It may well have become just another one of those self-congratulatory rhetorical devices that grace the public utterances of Anglo-American politicians. No intellectual effort need therefore be wasted on this bit of ruling-class chatter".

- Judith Shklar

This “ruling class chatter” forms a vital framework of law, but only when current legislation reflects its principles. It must be continually upheld, especially as its jurisdiction progresses into unprecedented territory. Cases such as Facebook-Cambridge Analytica show the growing value of mass user data and the general public’s ignorance of the extent their information can be collected, sold, and used. As surveillance is brought to the forefront of the collective public consciousness, the corresponding laws and regulations should also become as prevalent and accessible as social media itself. As stated by the Right Honorable Lord Bingham in his 2006 lecture, “if everyone is bound by the law they must be able without undue difficulty to find out what it is”. However, social media surveillance is progressing at a pace where law has not followed, creating weaknesses that compromise rule of law.

Rule of law is an “underlying constitutional principle”, forming the framework of law and its interactions with the people (Scott, 2013). It underpins the entire system, requiring all people, no matter their rank, to be held answerable to the same public courts. As a natural consequence, “the law must be accessible and so far as possible intelligible, clear and predictable” (Bingham, 2006). All bound by law, all are equal under the law, all can access and understand the law. These concepts boil down to three major principles: accessibility, clarity, and equality. Only when everyone can find and understand the law can they be effectively bound by it. This understanding takes “law” from the intangible into the mundane. It is crucially important to maintain these three principles, as if compromised, they erode the fairness of law, the accountability of the government, and the trust of the people. With social media and social media surveillance growing ever more prevalent, laws and regulations have failed ensuring those three principles. The Canadian government adversely affects the Rule of Law due to inaccessible and unpredictable regulations on social media surveillance.

Public access has become much easier with technology, but the RCMP’s Project Wide Awake is surprisingly under-publicized, despite its relevance to Canadians. It conducts both proactive and reactive monitoring of social media, without any information on what falls under scrutiny, or what

would require "proactive policing" (Carney, 2019). The project uses Social Studio, a software that claims to be a "fly on the wall" and allows the user(s) to "monitor multiple social accounts and topic profiles, monitor discussions from owned social accounts and broader social news" (Salesforce). However, their marketing statements don't paint a comprehensive picture of RCMP monitoring, nor should a Canadian citizen have to research the functionalities of an American software to understand their own laws. Although currently under internal audit, there is nothing accessible on whether its monitoring is ongoing, or any publication of regulations or restrictions on use (Tunney, 2019). The RCMP's statement on their use of the controversial Clearview AI facial recognition app is equally unclear, with "a few units in the RCMP" using it "on a trial basis with respect to criminal investigations" (Meyer, 2020). Yet this statement was only in response to Clearview AI's entire client list being stolen and publicized. Without that leak, Canadians would not know that their photos on social media were being analyzed, by an unknown number of units, for an unknown period of time. It was immediately put under investigation by the OPC, but "given the office is investigating, no further details are available at this time" (OPC, 2020). There is a distinct lack of transparency on the RCMP's use and collection of social media data, with important operational information made inaccessible to the public[1]. However, what information *is* available is neither predictable nor easy to understand.

Laws in Canada make provisions for a "reasonable expectation of privacy", supported with many physical examples in Section 8 of the Charter, but none digital. These reasonable expectations seem to change depending on the judge, with Justice Brown stating in in *Leduc* v. *Roman*, 2009: "A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile", but Justice Price in Schuster v. Royal & Sun Alliance Insurance Company of Canada, 2009 ruled in favor of the Plaintiff, who had "set her

[1] *Both Social Studio and Clearview AI are headquartered in the United States, so perhaps operating and data-collection systems would be unpredictable and inaccessible to those without access to their proprietary software.*

Facebook privacy settings to private and [had] restricted its content to 67 "friends", therefore proving that "she had not created her profile for the purpose of sharing it with the general public. Unless the Defendant establishes a legal entitlement to such information, the Plaintiff's privacy interest in the information in her profile should be respected." "Reasonable expectation of privacy" is no longer a reliable legal definition. Collection and use of social media data hinges on "public" or "open source" information, but it's becoming more and more evident that *all* information is public. Bill C-59 defines it as "any information that is published or broadcast for public consumption, but also any information that is accessible to the public on or off the Internet … and information that is available to the public upon request, by subscription or even by purchase*"* (Scotti, 2018). The bill works to exclude "Canadian citizens, permanent residents, Canadian corporations, anyone in Canada or at any portion of the global information infrastructure in Canada", but collecting incidental information is acceptable if Canadians weren't the initial targets (Parliament of Canada, 2019). This vagueness seems to imply that the CSE would be perfectly within its rights to obtain information from Canadians, as long as they aim slightly to the side. The CSE is directed "to ensure that measures are in place to protect the privacy of the aforesaid groups", without further clarification. It is difficult for the general public to understand how they and their data would be affected by Bill C-59. Existing terms are unclear and unpredictable, despite forming the legal framework for government surveillance. These overarching issues with government social media surveillance create a legal quicksand, where cases and Canadians may fall through the cracks.

Rule of law dictates that all are equal under the law, a tenet likely to be compromised by lack of accountability, caused by the inaccessible and unclear legislation so far. Public outcry for Colten Boushie, Cindy Gladue, and other high-profile cases involving Indigenous victims are only able to generate so much discussion and increased awareness due to the case being public knowledge, exposing institutionalized weaknesses within Canada's justice system. Accountability, privacy protection, and general education are only possible if procedures are visible, which "doesn't

work in a big data age, because its systems are invisible to us" (Vonn, 2019). With information on government surveillance and the impact of collected data on law enforcement being vague and insufficient, it creates an environment that perpetuates inequality. Like "other types of surveillance technologies, social media monitoring appears likely to disproportionately affect communities of color" (Levinson-Waldman, 2018). Many growing software and AI based tools for law enforcement are based off existing databases of information, including their historical overrepresentation of minorities. With Clearview AI lacking any "actual racial bias methodology" and Social Studio's system being unknown, the results of these tools may only magnify existing issues, and more easily pass under the radar due to the mistaken idea that software is objective (Thomson, 2018). Due to lack of publicly accessible information on social media surveillance, systematic discrimination may be directly uploaded into these tools for the 21st century. Having already identified systemic discrimination as a serious criminal justice issue, Canada should avoid potentially worsening inequality (Department of Justice, 2019).

There are clear weaknesses within the current system, weaknesses that adversely affect the rule of law. These issues of accessibility and clarity need to be rectified to prevent future consequences and to guide legislation in uncharted territory. One cannot pick and choose which areas to fix, as any one principle is useless on its own: accessibility is meaningless without understanding, equality is dysfunctional if inaccessible. Only in conjunction do they function as the backbone of our constitution. Only under an updated framework that considers the needs of the public with respect to social media surveillance can there be true rule of law, and not just empty words.

References

Bingham, T. (2006). *'The Rule of Law' Text Transcript.* Retrieved from University of Cambridge Centre for Public Law: https://www.cpl.law.cam.ac.uk/sir-david-williams-lectures2006-rule-law/rule-law-text-transcript

Carney, B. (2019, March 25). *'Project Wide Awake': How the RCMP Watches You on Social Media.* Retrieved from The Tyee: https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/

Department of Justice. (2019, November 4). *Department of Justice*. Retrieved from Understanding the Overrepresentation of Indigenous People in the Criminal Justice System: https://www.justice.gc.ca/socjs-esjp/en/ind-aut/uo-cs

Levinson-Waldman, R. (2018). Government Access to and Manipulation of Social Media: Legal and Policy Challenges. *Howard Law Journal Vol. 61 No. 3*, 525.

Meyer, C. (2020, February 27th). *National Observer.* Retrieved from RCMP admits it uses controversial Clearview AI facial-recognition app: https://www.nationalobserver.com/2020/02/27/news/rcmp-admits-it-uses-controversial-clearview-ai-facial-recognition-app

OPC. (2020, February 28). *Office of the Privacy Commissioner of Canada.* Retrieved from OPC launches investigation into RCMP's use of facial recognition technology: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/

Parliament of Canada. (2019, June 21). *Parliament of Canada.* Retrieved from Bill C-59: https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent

Salesforce. (n.d.). *Here's everything you need to know about social media monitoring.* Retrieved from Salesforce: https://www.salesforce.com/products/marketing-cloud/best-practices/social-media-monitoring/

Scott, S. A. (2013, February 7). *The Canadian Encyclopedia.* Retrieved April 29, 2020, from Rule of Law.

Scotti, M. (2018, February 6). *Here's what you need to know about Canada's 'extraordinarily permissive' new spying laws.* Retrieved from Global News: https://globalnews.ca/news/3999947/cse-c59-new-spy-powers-canada/

Thomson, S. (2018, September 24). *CBC* . Retrieved from 'Predictive policing': Law enforcement revolution or just new spin on old biases? Depends who you ask: https://www.cbc.ca/news/world/crime-los-angeles-predictive-policing-algorithms-1.4826030

Tunney, C. (2019, November 05). *CBC.* Retrieved from RCMP launches review of its social media monitoring operation: https://www.cbc.ca/news/politics/rcmp-social-media-review-1.5346741

Vonn, M. (2019, March 26). *The Tyee.* Retrieved from RCMP's Social Media Surveillance Symptom of Broad Threat to Privacy, Says BCCLA: https://thetyee.ca/News/2019/03/26/RCMP-Surveillance-Threat-Privacy/