The follow are a set of extended excerpts from "Grim Realities of Life in Canada - Section 8"

1. **First set of incidents:**
   Throughout October 2019, the camera's flash on my phone would automatically turn on in flashlight mode and stay on, whenever a police cruiser would go by my home and blare its siren for a brief moment, just as it passed by my apartment building on 310 Queen Street South, Kitchener. This would happen three to four times a week, late at night, between 10 pm and 3 am. This was precisely consistent, each time, with the police siren blaring for a moment right outside my bedroom's window, which faced Queen Street on the first floor of the building.

   Such belligerent and repeated violations of my peace were deliberate scare tactics aimed at startling and frightening me while using tortuous methods designed to cause sleep deprivation, fear, and agitation. These kinds of subtle, psychological tools that conveniently leave no trace of being deployed by — the police and their supervisors — were used for causing terror, for antagonising innocent civilians, for depriving people of their quiet enjoyment of an unspoiled home and neighbourhood environment, and for deeply disrupting a targeted person's mental peace and wellness.

   It was evident to me that an individual police officer, or a group of local police officers on patrol were able to use their vehicle’s equipment to communicate with my phone via the push-notification-module of the emergency-services-system-library of Android-OS. This method of communication is controllable by first responders. However, its usage requires a legal warrant or an actual emergency situation like a natural disaster or an abduction associated with an amber alert. This is how an emergency communication channel strictly reserved for search and rescue operations was abused for harming vulnerable individuals in a targeted manner.

   The more heinous issue was that the same tactic was being used against orphaned and homeless youngsters who had taken refuge in the youth shelter next to my apartment building, which was called **One Roof.** Based on my interactions with a number of youth from the shelter, I can say with certainty, that the police had abused and harassed those disenfranchised homeless individuals, to scare and drive them away from One Roof on Queen Street, Kitchener, Ontario.

   Two months after these continued harassment drove people away from the shelter, it was

opportunistically demolished by Vive Development company to give way to a new apartment complex. This was a strong indication that a local real estate development group with its contractors, had employed *dirty police officers* to clear the location's legitimate users, before taking over the land.

It can be observed that the very label of, "at risk individual," ascribed by social or policing services to individuals already suffering from misfortune, was being ruthlessly used as an identifier for targeting vulnerable people by officers from those public services charged with the duty of care for protecting and supporting them.

This is the day-to-day reality of corruption in Kitchener, Ontario, Canada where the police are wielded by business dons to drive away minorities, refugees, orphans, meak and huddled homeless people, as well as persons of colour — for the sake of personal gains and profiteering through the abuse of publicly vested authority.

In this tragic case, how will the youth that were terrorised and chased away using overt and covert methods of harassment ever be recognized and compensated?

2. **Second set of incidents:**
   Also in October 2019, the indicator for my phone's GPS location services would turn on for a few seconds, each time I would turn on my phone's WiFi. This was confirmed by my wife and I, on numerous occasions throughout October 2019. If I turned on the phone's WiFi outside my home this issue would not happen. At home, I removed the SIM card and tried toggling the WiFi, and the phone would still automatically turn on the location for a few seconds.

   This was a sufficient indication and a cause for concern that a digital hacking tool had been used against my phone to collect data on my location and whereabouts. This type of a sophisticated cybercrime is very difficult to conduct on a Samsung Android phone as it requires a method to circumvent the phone's manual user inputs as well as other fail safe settings in the phone that prevent the leakage of its GPS location.

   I knew that such geo-tracking methods could be perpetrated using cyberwarfare tools available to secret services of The Five Eyes intelligence group because of my professional R&D work in the area of computer networks and digital security. Hence, a feeling of deep dismay due to severe violations against my privacy began around this time in 2019.

Being tracked by groups that could exert such brute force via cyberwarfare tactics and malicious digital tools against persons like myself, greatly upset me. It also hampered my work and harmed my well being. This act of betrayal of my trust showed a complete lack of good faith by various authorities, because of the way they injuriously surveilled my home, personal and private affairs, movements, and communications for reasons, which were never told to me or brought to my attention through a formal and straightforward written notice.

3. **The third set of incidents:**
   In the second week of November 2019, the day after I happened to mention during a peer-support group meeting, that I was in possession of various evidence about the involvement of U.S. led soldiers in war crimes committed in Afghanistan and Iraq, my personal computers were hacked. And the particular folder containing the evidence was tampered with. The folder included names and affiliations of individuals from American, British and Canadian origins. It showcased the details of their method of committing mass murder of civilians in Afghanistan and Iraq from 2003 to 2010.

   Also, according to news media outlets, those mass killings of civilians via aerial drones, as well as incidents of rapes and torture of Afghan civilians by US led troops and their contractors, particularly by Australian ones, had continued throughout the period of 2010s and into 2020s.

   The place where I had attended the peer-support group meeting and spoken about having such evidence was a private location where, "trust was of paramount importance." I believe that the cyberattack, which completely violated my trust and privacy, could have only been carried out via the help of trained intelligence units with local authority and jurisdiction. These units demonstrated their stance and position of animosity and hostility against me by defiling my personal security, and by aggressing against my life using covert and coordinated means of hostile attacks using cyberwarfare tools.

   As such, the instigating intelligence or secret service units that desecrated the sanctity of the only remaining physical and online safe spaces available to me, opened themselves as well as the policing and private companies aiding them, to justified retaliations.

   One may argue that in this particular case I am expressing a selective bias towards ascribing malice to American, Canadian or British intelligence and secret service units by connecting

two possibly unrelated events — the first event, where I happened to mention the digital location of a copy of sensitive material in my possession at a private venue and the second event, where I discovered on the next day of the first event that only the particular set of digital folders, containing the afore-mentioned sensitive information, were hacked into by an assailant.

Couldn't it be that a generic hacker, not connected to any of the Five Eyes intelligence group or other secret services was lurking in my computer networks, who then chanced upon a folder that seemed lucrative enough to steal?

This is unlikely because there was another folder location in the same computer network that contained other pieces of information connected to the hacked folders, which remained untouched. And I do believe this was because I did not mention anything about the second set of folders outloud during the peer-support meeting. A generic hacker sifting through all files in my computers looking for things that contained anything about Afghanistan, drones, or war crimes would have found and taken those additional files as well.

All of these incidents deprived me of health and mental peace, and forced me to divert my resources towards rebuilding my computer networks as well as painstakingly resetting my phone's firmware. The incidents explained in this section also caused me to lose the opportunity to work on my private company, to follow up on pitches for venture capital to potential investors, and to service ongoing business operations.

These losses were severe as I was hindered and diverted from being able to follow up with potential investors and investment groups for building the startup, and from maintaining existing business relationships.

The hacking incidents also violated and breached the privacy of my clients' data that was securely protected within my company's computer network and online account. It also jeopardised the intellectual property vested in my company and diminished the equity of the company's employees while also breaching the privacy of their private and protected data.

These assaults upon my peace, private properties, relationships and health caused a further loss of earnings and income over the subsequent years. The more disheartening and disappointing loss was in not being able to utilise the company's main intellectual property to perform services

for elderly care and for persons with different forms of dementias or memory challenges. Such opportunity costs have been considerably high.

The issues highlighted in this section of the overall chain of events are indicative of a systemic fault within the region's policing and judiciary services that unnecessarily targets, molests, and harrasses persons it unfairly characterises as being ``suspicious, vagrant, derelict, or `at risk` of becoming a burden or a threat to society.`` Worse, their wrongdoings are perpetrated using menacing and terrorising tools, techniques, strategies, and tactics of cyberwarfare.

