RCMP Project Wide Awake: Government Surveillance and Invasion of Privacy

In March 2019, The Tyee newspaper published an article on the RCMP's use of online social media surveillance. The RCMP claimed that "Project Wide Awake" surveillance was through open source tools (tools publicly available to anyone), and was only collecting publicly available social media information.

In November 2020, The Tyee began publishing further articles on the tools and techniques the RCMP uses. These reports show that not only does the RCMP go beyond open-source to invade our privacy for "proactive" law enforcement, they hide the powerful tools used to do so, because telling the truth might make us more private, and that would make it harder for them to invade our privacy.

Gathering Publicly Available Information

Originally, The Tyee reported that RCMP Spokesperson Sgt. Tania Vaughn claimed they only used open source information for "proactive" monitoring, and there was no mass surveillance used nor private information being read (Carney 2019).

The RCMP would not release information on policies or activities, and refused to share their privacy assessment. Unsurprisingly, the RCMP's unproven promises weren't enough to mollify reporters or watchdog organizations like Citizen Lab and the Canadian Civil Liberties Association.

Private Public Information

Christopher Parsons of Citizen Lab (the internet-security focused section of University of Toronto's Munk School of Global Affairs and Public Policy) explained in both the March 2019 article in The Tyee and later to the CBC (Tunney 2019) that just because a person posts to a public site, they can still expect a level of privacy regarding the government.

In an offline "real world' example, in **Vanderveen v Waterbridge Media Inc. (2017)** the judge decided that just because a person is in public, an organization can't just use their image.

In much the same way, there must be a *reason* for the police, as the government, to bypass privacy and act on our information. And *usually* we should be informed of why.

Private Information of Public Interest

"The *Privacy Act* in brief" on the Office of the Privacy Commissioner of Canada's (OPC) website states that "Canadians need to know that their personal information is being collected and used only according to strict rules that preserve their right to privacy," and this applies to use for public safety and federal policing (OPC 2019).

When The Tyee wanted to know more about what the RCMP was doing as a matter of public interest, they required Freedom of Information (FOI) requests to get answers. The many months between the first story and these recent ones was due to waiting for those requests to be filled.

The RCMP obviously cannot wait like that when it's a matter of urgent need—public safety sometimes requires quick access to private information. But, as Citizen Lab's Kate Robertson explained to The Tyee, the RCMP is subject to judicial oversight: They need a reason and judicial permission to gather private information, and that permission can't just be "in case" they find something they can act on (Carney 2020).

Uncovering Private Data (Ours and the RCMP's)

After the FOI release, it became obvious why the RCMP would not share their assessments with The Tyee or watchdog organizations: it goes out of its way to gather data that we work to keep secure. The organization purchases specialized investigative tools to bypass privacy settings and gather information hidden from social media feeds. It also goes to great effort to hide the existence of the tools used from judicial review and public records, claiming national security needs should mean they aren't required to get permission (Carney 2020).

The argument seems to be that if we knew how and where it gained intelligence, we would take further steps to keep private information more private, which would limit mass surveillance. Instead of an arms race, individuals would be in a privacy race with their own government.

Edited

RCMP Project Wide Awake: Government Surveillance and Invasion of Privacy

In March 2019, The Tyee newspaper published an article on the RCMP's use of online ~~social media~~ surveillance. The RCMP claimed that "Project Wide Awake" ~~surveillance was through~~used open-source tools (tools ~~publicly~~ available to anyone), ~~and was only~~to collect~~ing~~ publicly available social media information.

In November 2020, The Tyee ~~began~~ publish~~ed~~ing further articles on the RCMP's tools and techniques ~~the RCMP uses~~. These reports show that ~~not only does~~ the RCMP ~~go beyond open-source to~~ invades our privacy~~, for "proactive" law enforcement, they~~ and hides the powerful tools used ~~to do so, because telling the truth might make us more private, and that would~~so we don't then make it harder to do ~~for them to invade our privacy~~.

~~Gathering~~ Publicly Available Information

Originally, ~~The Tyee reported that~~ RCMP Spokesperson Sgt. Tania Vaughn claimed the RCMP~~y only~~ didn't use mass surveillance nor private information ~~used open-source information~~ for "proactive" monitoring~~, and there was no mass surveillance used nor private information being read~~ (Carney 2019).

However, t~~T~~he RCMP would not release information on "proactive" policies~~, or~~ activities, ~~and refused to share their~~or privacy assessments. Unsurprisingly, the RCMP's ~~unproven~~ promises ~~weren't enough to~~did not mollify reporters or watchdog organizations ~~like Citizen Lab and the Canadian Civil Liberties Association~~.

Private Public Information

Christopher Parsons of Citizen Lab (the internet-security focused section of University of Toronto's Munk School of Global Affairs and Public Policy) explained ~~in both the March 2019 article into~~ The Tyee and ~~later to the~~ CBC News ~~(Tunney 2019)~~ that ~~just because~~even when a person posts to a public site, they can still expect a level of privacy ~~regarding~~ from the government (Carney 2019, Tunney 2019).

In an offline "real world" example, in **Vanderveen v Waterbridge Media Inc. (2017)** the judge decided that an organization can't use a person's image just because they are~~a person is~~ in public~~, an organization can't just use their image~~. ~~In much the same way~~Similarly, ~~there must be a *reason* for the police,~~ as the government, the police need a *reason* to ~~bypass privacy and~~ collect and act on our information. ~~And *usually* we should be informed of why.~~

Private Information of Public Interest

"The *Privacy Act* in brief" on the Office of the Privacy Commissioner of Canada's (OPC) website states that "Canadians need to know that their personal information is being collected and used only according to strict rules that preserve their right to privacy," and this applies to use for public safety and federal policing (OPC 2019).

~~When The Tyee wanted to know more about what the RCMP was doing as a matter of public interest, they required Freedom of Information (FOI) requests to get answers.~~ Even as a matter of public interest, The Tyee had to submit Freedom of Information (FOI) requests to learn more about the RCMP's private activities. ~~The many months between the first story and these recent ones was due to waiting for those requests to be filled.~~The newspaper waited over a year for the FOI release.

The RCMP obviously cannot wait ~~like that~~that long when it's a matter of urgent need—public safety sometimes requires quick access to private information. But, as Citizen Lab's Kate Robertson explained to The Tyee, the RCMP is subject to judicial oversight: They need ~~a reason and judicial~~ permission to gather private information, and ~~that permission~~ the reason can't ~~just~~ be "in case" they find something they can act on (Carney 2020a).

~~Uncovering~~ Private Data (Ours and the RCMP's)

After the FOI release, it became obvious why the RCMP would not share their assessments ~~with The Tyee or watchdog organizations~~: it ~~goes out of its way to~~actively accesses data that ~~we~~ Canadians work to keep secure. The organization purchases specialized ~~investigative~~ tools to bypass privacy settings and gather information hidden from social media feeds. It also ~~goes to great effort to~~ routinely hides the existence of these tools ~~used~~ from judicial review and public

RCMP Project Wide Awake: Government Surveillance and Invasion of Privacy

In March 2019, The Tyee newspaper published an article on the RCMP's use of online surveillance. The RCMP claimed that "Project Wide Awake" used open-source tools (tools available to anyone) to collect public social media information.

In November 2020, The Tyee published further articles on the RCMP's tools and techniques. These reports show that the RCMP invades our privacy, and hides the powerful tools used so we don't then make it harder to do.

Publicly Available Information

Originally, RCMP Spokesperson Sgt. Tania Vaughn claimed the RCMP didn't use mass surveillance nor private information for "proactive" monitoring (Carney 2019). However, the RCMP would not release information on "proactive" policies, activities, or privacy assessments. Unsurprisingly, the RCMP's promises did not mollify reporters or watchdog organizations.

Private Public Information

Christopher Parsons of Citizen Lab (the internet-security focused section of University of Toronto's Munk School of Global Affairs and Public Policy) explained to The Tyee and CBC News that even when a person posts to a public site, they can still expect a level of privacy from the government (Carney 2019, Tunney 2019).

In an offline "real world" example, in **Vanderveen v Waterbridge Media Inc. (2017)** the judge decided that an organization can't use a person's image just because they are in public. Similarly, as the government, the police need a *reason* to collect and act on our information.

Private Information of Public Interest

"The *Privacy Act* in brief" on the Office of the Privacy Commissioner of Canada's (OPC) website states that "Canadians need to know that their personal information is being collected

and used only according to strict rules that preserve their right to privacy," and this applies to use for public safety and federal policing (OPC 2019).

Even as a matter of public interest, The Tyee had to submit Freedom of Information (FOI) requests to learn more about the RCMP's private activities. The newspaper waited over a year for the FOI release.

The RCMP obviously cannot wait that long when it's a matter of urgent need—public safety sometimes requires quick access to private information. But, as Citizen Lab's Kate Robertson explained to The Tyee, the RCMP is subject to judicial oversight: They need permission to gather private information, and the reason can't be "in case" they find something they can act on (Carney 2020a).

Private Data (Ours and the RCMP's)

After the FOI release, it became obvious why the RCMP would not share their assessments: it actively accesses data that Canadians work to keep secure. The organization purchases specialized tools to bypass privacy settings and gather information hidden from social media feeds. It also routinely hides the existence of these tools from judicial review and public records, claiming national security means it shouldn't need permission (Carney 2020a, Carney 2020b).

The RCMP believes that if we knew how and where it gained intelligence, we would take steps to keep private information more private, which would limit mass surveillance. Instead of an arms race, individuals would be in a privacy race with their own government.

"Proactive" Surveillance

While using these resources for investigating "Darknet" (encrypted information) activities, the RCMP includes private conversations and political activity (Carney 2020a). The RCMP spies on people, in case they may have online social contacts who might later commit crimes.

The example of "proactive" use Sgt. Vaughan gave The Tyee should be recognizable in its danger: the RCMP can monitor private communication looking for legal protest organizing "in