Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PR20-00027

Ministry of the Solicitor General

September 15, 2021

Summary: This investigation file was opened after the Ministry of the Solicitor General (the ministry) contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report a privacy breach under the *Freedom of Information and Protection of Privacy Act*. The breach related to the ministry's look-up tool web portal for COVID-19 status information (the Portal). Specifically, the ministry advised that an audit of the Portal had determined that a number of police services had conducted broad ranging community searches rather than performing a more specific search of individuals tested for COVID-19.

This report concludes that the ministry did not have adequate measures in place to protect the personal information contained in the Portal. It also finds that the ministry did not respond adequately to the breaches.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*

Orders and Investigation Reports Considered: PR16-40, PC11-34

BACKGROUND:

[1] On April 13, 2020, as part of the Ontario Government's response to the COVID-19 pandemic, an order was made under the *Emergency Management and Civil Protection Act* (the *EMCPA* order), pursuant to which the Ministry of the Solicitor General (the ministry) developed a look-up tool web portal for COVID-19 status information (the Portal) and provided first responders throughout Ontario access to it from April 13, 2020 to July 22, 2020. The Portal provided information about the COVID-19 status of specific individuals, including their name, address, date of birth, and test result. Although the

database was later amended to only include confirmed positive results, initially, individuals with pending test results were also listed in the Portal.

[2] On July 15, 2020, the ministry contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report a privacy breach under the *Freedom of Information and Protection of Privacy Act* (the *Act*). Specifically, the ministry advised that an audit of the Portal had determined that a number of police services had conducted broad ranging community searches rather than performing more specific searches of individuals tested for COVID-19.

[3] In response to a request from this office, the ministry provided a spreadsheet with what they described as a redacted[1] copy of the audit results. The audit results spreadsheet included fields for the search date, the name of the Police Service and the user's name. The audit results spreadsheet also included fields for the search parameters (name, address, municipality and postal code), with the fields being populated with the search parameters that were entered by the particular user.

[4] On August 17, 2020, the Canadian Civil Liberties Association (CCLA) issued a press release explaining that data it obtained from the Ministry of the Attorney General showed that, during the time the Portal was active, Ontario police had accessed the portal over 95,000 times. After reviewing the ministry's breach report and what appeared to be a disproportionately high number of searches, the IPC had concerns regarding whether the Portal was being used properly and in accordance with the *Act*.

[5] In light of the above information, the IPC wrote to the ministry[2] and to a number of police services requesting information in relation to their searches of the Portal.

[6] After reviewing the responses as well as the audits, the IPC still had concerns about how searches of the Portal were being conducted. As a result, this matter was streamed to the investigation stage of the IPC's complaint process, and I was assigned as the Investigator.

Transfer to Investigation Stage at the IPC:

[7] As part of my investigation, I reviewed the information provided at the Intake Stage and determined I required additional information. I then wrote to the ministry and several police services and asked further questions about the Portal. I also wanted information regarding what had been communicated to staff about Portal searches, and what steps had been taken to ensure reasonable measures were in place to prevent unauthorized access to the personal information in the Portal.

[8] Information received from the police services and the ministry, as well as my own

---

[1] According to the ministry, they redacted the personal information of the "individuals that appeared in the database".
[2] The OPP is part of the Ministry of the Solicitor General.

conclusions with respect to this matter, are set out in this Report.

ISSUES:

I identified the following key issues in this investigation:

1. Is the information at issue "personal information", as defined by section 2(1) of the *Act*?

2. Did the ministry have reasonable measures in place to prevent unauthorized access to the personal information in the Portal in accordance with section 4(1) of Regulation 460 of the *Act*?

3. Did the ministry respond adequately to the breaches?

DISCUSSION:

RESULTS OF INVESTIGATION:

ISSUE 1: Is the information at issue "personal information", as defined by section 2(1) of the Act?

"Personal information" is defined in section 2(1) of the *Act*.

Section 2(1), in part, states:

> "personal information" means recorded information about an identifiable individual, including,
>
> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> c) any identifying number, symbol or other particular assigned to the individual,
>
> d) the address, telephone number, fingerprints or blood type of the individual,
>
> …

> h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[9] At issue is the information contained in the Portal. The information includes the name, address, date of birth, and COVID-19 test result.

[10] Based on the above definitions, I am satisfied that all of the information at issue qualifies as "personal information" under the *Act*. The ministry does not dispute this.

[11] Therefore, I find that the information at issue is "personal information" as defined by section 2(1)(b) and (h) of the *Act*.

ISSUE 2: Did the ministry have reasonable measures in place to prevent unauthorized access to the personal information in the Portal in accordance with section 4(1) of Regulation 460 of the Act?

Section 4(1) of Regulation 460 of the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[12] In Privacy Complaint Report PR16-40, I stated the following regarding section 4(1) of Regulation 460 of the *Act*:

> From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.
>
> Furthermore, simply because a breach occurred does not by itself mean that reasonable measures were not in place. The standard set out in section 4(1) is not perfection but reasonableness. It is therefore possible for records to be accessed in an unauthorized manner and yet the measures in place still be reasonable.

[13] Further, in Privacy Complaint Report PC11-34, this office stated the following:

> The requirement to put in place reasonable measures to protect information from unauthorized access pursuant to section 4(1) includes a requirement to ensure that staff are appropriately trained in the management of personal information. This means that staff and management who require access to

> personal information in order to perform their duties shall receive training to a level commensurate with the sensitivity of the information to which they have access.

[14] In the circumstances of this matter, I agree and adopt the reasoning set out above.

[15] The records at issue in this breach are the electronic test results of individuals who were tested for COVID-19 as well as their name, address, and date of birth. In my view, this type of information, particularly the test results, would be considered sensitive personal health information and I have found that this information qualifies as personal information under the *Act*.

[16] Accordingly, it is reasonable to expect that before providing access to this type of information, the ministry would have put measures into place to prevent unauthorized access to the personal information of individuals not subject to a call for service.

[17] The ministry has explained that access to the Portal was restricted to select authorized users responsible for call taking/dispatching and described the security measures in place to protect the security systems containing the data, to ensure only those authorized had access to the Portal. The ministry also advised that an audit function was instituted to track all authorized users' activity on the Portal.

[18] The ministry reported that during an audit of the Portal's use, it discovered that staff were conducting "broad based" searches instead of specific searches for individuals who were subject to calls for service, contrary to the ministry's instructions regarding the use of the Portal. The ministry explained that the broad based searches of concern were performed by entering one field such as postal code, municipality, city, full names and/or last names matching authorized users. Some searches included both the municipality and postal code.

Administrative Measures and Safeguards

Training

[19] During my investigation, I asked the ministry how staff were trained on the use of the Portal and who was training them. In response the ministry advised that:

> On April 11, 2020, instructions specific to the access of information to MOH COVID-19 portal were provided by the Ministry of the Solicitor General and disseminated to all PCC members. The dissemination of information included the All Chiefs Memorandum 20-0044, the MOH COVID-19 search user guide and the PCC Standard Operating Policy excerpt regarding the use of non-OPP resources.

[20] I understand however, that the following All Chiefs Memos in relation to the Portal were also sent to the police services in regards to the Portal.

Memo 20-0041	Disclosure of COVID-19 Status Information by Laboratories and Public Health Units (April 6, 2020)
Memo 20-0044	Authorized Users for Disclosure of COVID-19 Status Information to Communication and Dispatch Centers (April 9, 2020)
Memo 20-0048	Launch of the First Responders COVID-19 Risk Look-Up Web Portal (April 13, 2020)
Memo 20-0064	First Responders COVID-19 Risk Look-Up Tool Web Portal: Protection of Personal Health Information and Appropriate Use (April 27, 2020)
Memo 20-0091	Audit of the First Responders COVID-19 Risk Look-Up Tool Web Portal (June 11, 2020)
Memo 20-0112	Expiry of Emergency Order, O.Reg. 120/20 (access to COVID-19 Status Information by Specified Persons) (July 20, 2020)

[21] These documents were provided to this office and I have reviewed each of them.

[22] Memo 20-0041 dated April 6, 2020, advises that the ministry is working with the Ministry of Health to develop an information Portal that would enable police services to query COVID-19 status information. It also states the following, in part:

> The ministry recommends chiefs of police centralize access to COVID-19 status information through their communications and dispatch service…access to information within police services should be limited to the greatest extent possible.
>
> …
>
> The ministry recommends police services boards and chiefs of police institute polices and procedures that prohibit access to COVID-19 (positive) status information at the conclusion of the provincial emergency and ensure destruction of the information as soon as permitted by law.
>
> …
>
> …chiefs of police should develop procedures on the access to and disclosure of such information, including the need for the supervisor of the police communication and dispatch services to ensure that information is only disclosed within the police service for the protection of officer safety when they are on route to specified calls for service.
>
> …

[23] The memo also attached a document titled "Call taking and Dispatching Protocols

for COVID-19 coronavirus" which listed a number of screening questions and set out how to document the responses.

[24] Memo 20-0044 dated April 9, 2020, includes information regarding the development and purpose of the Portal, retention, disclosure and security of the information and describes who should be an authorized user.

[25] Memo 20-0048 dated April 13, 2020, describes how access to the Portal will only be provided to authorized users, and that "information shared pursuant to the emergency order only be used to prevent, respond to or alleviate the effects of the emergency…" It also states that "having access to COVID-19 status information is only one tool to assist frontline personnel when taking appropriate precautions…" and "for more information, on the limitations of the information in the Portal, please refer to the user guide provided to authorized users".

[26] Memo 20-0064 dated April 27, 2020, describes what information is contained in the Portal and explains that the Portal is "only intended to be used to look up the COVID-19 status of individuals that members of the police service will encounter or have encountered during the declared emergency as a result of responding to calls for service…" and also states that searches "should not be conducted to ascertain the number of individuals in a municipality or region that appear on the portal…such use of the portal is not consistent with the requirements of the EMCPA."

[27] This memo also includes a description of the audit logging function which advises that:

- the Portal included an audit logging function that tracked all user activity on the portal and may flag queries that are deemed to be an inappropriate use of the portal (e.g., broad municipal-based searches);

- if inappropriate use of the portal is confirmed, the ministry may revoke access and "may report suspected unauthorized portal access or use/disclosure of information from the portal to the IPC;

- police services boards and chiefs of police should commence their own internal investigation and, where appropriate undertake disciplinary measures for all unauthorized access, or use or disclosure of information from the portal; and

- on request of a chief of police or police services board, the ministry will provide a copy of an authorized user's audit logs for the purpose of investigating, unauthorized access, or use or disclosure of information, for the purpose of pursuing discipline.

[28] Lastly, this memo includes details regarding the retention and record-keeping of the information contained in the Portal and an FAQ about the Portal. I note that the FAQ provides contact information if the need for a user's activity log arises and specifically states that the audit logging function "will track all user activity on the portal and flag any

queries that are deemed to be inappropriate…"

[29] On June 11, 2020, Memo 20-0091 was issued. This memo provides information related to the audits and advises that "many searches of the portal do not appear to be consistent with the ministry's instructions or the restrictions on the use of the information subject to O. Reg. 120/20[3]…" It contained a reminder regarding the appropriate use of the Portal and provides examples of the types of searches that are not consistent with the ministry's instructions and included broad based searches and searches for specific names not related to an active call for service. It also indicated that searches outside the service area are not appropriate.

[30] Memo 20-112 dated July 20, 2020, advises of the expiry of the Emergency Order and that the Portal will be discontinued (and all authorized users accounts will be deactivated), effective July 20, 2020. This memo also states the following:

> Please note that the [ministry] will be preserving records of the portal's usage in accordance with applicable law. The ministry will work with police services boards and chiefs of police to make the necessary records of usage available to support any employment disciplinary measures related to ensuring the appropriate use of the portal or investigation into potential privacy breaches."

Using the First Responder COVID-19 Risk Look-Up Tool (the guide)

[31] As previously indicated, the ministry's training consisted of providing the above noted Guide to staff as well as a number of All Chief Memos which related to the Portal. The ministry did not provide any further training material. I have reviewed the Guide and among other things, the Guide includes information regarding:

- the appropriate use of the Portal;
- the retention, disclosure and security of the information contained in the Portal;
- setting up an account; and
- how to use the Portal.

[32] I note that the examples provided in the Guide are all searches where only one field has been entered. For instance, the first example demonstrates entering only a last name and notes "You can search using any field…" The second example uses the city of Toronto as an example and states the following, "In this example, entering "toronto" returns multiple pages of search results. A maximum of 5 results will be displayed on each page. To scroll through all results, click on the "Right Arrow". Results are sorted by

[3] *Emergency Management and Civil Protection Act*, Ontario Regulation 120/20 Access to Covid-19 Status information by Specific Persons.

…."

[33] Lastly, I note that the Guide states the following:

> Wildcard Search Strategy
>
> Due to the data quality gaps noted previously, you may use "Wildcards" to maximize your search results in the COVID-19 status information database. A "Wildcard" is an advanced search technique used in search terms to represent one or more other characters. An asterisk (*) may be used to specify any number of characters. It is typically used at the end of a root work or phrase.

[34] The Guide then demonstrates this type of search strategy.

[35] In addition to the above, and in response to questions posed by this office, the OPP, which is a part of the ministry advised that "It should be noted that when the instructions on usage of the portal were provided, broad based searches were demonstrated as a method of attempting to locate a person who tested positive for COVID-19".

[36] The searches used as instructional examples in the Guide which only require that one field be populated are, in my view, the type of broad based searches which the ministry later described as improper uses of the portal. For example, the Guide provided search examples where only a postal code or municipality was entered, whereas Memo 20-0091, stated the following, in part:

> As a reminder, the following examples of the portal usage are not consistent with the ministry's instructions or the restrictions on the use of the portal:
>
> • Conducting broad-based municipal searches without a specific address, including broad-based searches using only postal codes. These types of municipal-wide searches have the potential to return a high number of response records, It is expected that authorized communications and dispatch personnel will only query the portal with other parameters in relation to an emergency call as opposed to searching an entire municipality
>
> ....
>
> • Conducting searches of a specific name that is not related to an active call for service.

[37] In my view, conducting searches such as these could potentially produce the personal information of individuals who were not subject to a call for service. For instance, conducting a search with only a postal code would produce a list that would include every individual in the Portal (that had a COVID test) that lives in that postal code.

[38] As indicated above, the Guide conflicted with what the ministry communicated in a number of their All Chief Memos.

[39] Based on the ministry's response, no additional training was provided and no other policies or procedures about the Portal were provided to this office. In my view, providing a guide and a policy to staff does not amount to training. As the gatekeepers for the Portal, it was the ministry's responsibility to ensure staff received consistent information about how the Portal should be used, and understood why a broad based search might result in a breach of privacy. This could have easily been accomplished with better training, specifically privacy training.

[40] In addition to the above, the ministry also provided information regarding the electronic safeguards in place, which included an audit logging function[4] as well as other security measures regarding passwords and user authentication.

Audit Logging Function

[41] As indicated previously, and according to Memo 20-0064, the ministry instituted an audit function that would track user activities and assist in investigations regarding unauthorized access, use or disclosure of personal information in the Portal. However, during my investigation, I learned that the audit logs provided to the police services did not include details regarding whose information was produced when the broad searches were conducted.

[42] To be clear, although the audit function had the capability of producing details such as whose personal information appeared in the results of the search, the ministry chose not to provide that information in the audit logs provided to the police services.

[43] The ministry explained that "…The audit logs do not contain the personal health information of individuals. It is a log of the search activity that allows managers to investigate the appropriateness of the portal access and it has been successfully used for that purpose."

[44] While I don't disagree that this type of audit log is helpful in determining whether a search of the Portal was broad and not in line with how a search should be performed, it falls short of providing the information necessary to determine whether or not a breach occurred. In addition, this limited information would not inform someone investigating a potential breach of the scope of the breach (how many individuals are affected), or details regarding who should be notified.

[45] Based on the information provided to me about the training and administrative safeguards, I find that the ministry did not have reasonable measures in place to prevent unauthorized access to the personal information in the Portal in accordance with section

[4] I have not provided details about the other safeguards for security reasons and because it is not necessary for the purposes of this Report.

4(1) of Regulation 460 of the *Act*.

[46] In my view, the ministry's lack of training, conflicting examples, and confusing communications contributed to the practice of broad based searches by users. In addition, the ministry's practice of providing limited information to the police services in relation to the audits, restricted police services' ability to conduct proper investigations to determine whether a breach of the *Act* occurred and who might be affected.

ISSUE 3: Did the ministry respond adequately to the breach?

[47] According to the ministry, the Portal was intended to be used to look up the COVID-19 status of individuals whom first responders may encounter or had encountered, as a result of responding to calls for service. The sole purpose was to support frontline personnel in making informed decisions about whether they needed to take additional precautions to prevent the spread of COVID-19. On July 20, 2020, in anticipation of the expiration of the *EMCPA* order on July 22, 2020, the Portal was decommissioned.

[48] In a letter dated November 26, 2020, the ministry provided our office with additional information about the breach and their response to it, which I have summarized below.

[49] After conducting an audit of the Portal and discovering that broad based searches were being conducted, the ministry implemented its privacy breach protocol and issued All Chiefs Memo 20-0091 dated June 11, 2020. As previously indicated, this memo provided information related to the audits and advised that "many searches of the portal do not appear to be consistent with the ministry's instructions or the restrictions on the use of the information subject to O. Reg. 120/20[5]…"

[50] The ministry's communication contained a reminder regarding the appropriate use of the Portal. It also provided examples of the types of searches that were not consistent with the ministry's instructions, such as broad based searches, searches for specific names not related to an active call for service, and searches outside the service area.

[51] After receiving the above noted communication, some police services requested their respective audits. The ministry also notified specific police services of any inappropriate queries conducted after the memo was issued. The ministry advised this office that the police services "should be responsible for any notifications to affected individuals."

[52] In terms of remedial action taken, the ministry stated the following:

---

[5] *Emergency Management and Civil Protection Act*, Ontario Regulation 120/20 Access to Covid-19 Status information by Specific Persons.

> The ministry instituted an audit logging function that tracked all user activity on the Portal and flagged any queries that were deemed to be an inappropriate use of the Portal (e.g., broad municipal-based searches).
>
> The ministry reported suspected unauthorized Portal access or use/disclosure of information from the Portal to the Information and Privacy Commissioner of Ontario.
>
> On July 20, 2020 the ministry shutdown the Portal and on July 22, 2020 Emergency Order O. Reg. 120/20 was revoked.
>
> Throughout this outbreak, we have called upon first responders to put their lives on the line every single day to protect Ontarians at great personal risk of being directly exposed to COVID-19. With their safety and health in mind, the government put in place an emergency order that temporarily enabled first responders to obtain COVID-19 positive status information about individuals with whom they were coming into direct contact.
>
> As the province continues to respond to this evolving pandemic, the government did not renew this time-limited emergency order. Effective Monday July 20th, access to COVID-19 status information and the portal was no longer available to first responders.
>
> The protection of personal health information remained a key commitment throughout this order. Recognizing that the local needs and challenges of individual communities across Ontario is varied, police and fire services were expected to implement local policies to ensure appropriate use and to take appropriate action in the case of misuse. Police and fire services are responsible for their use of the portal within the requirements of the emergency order.
>
> Once again, the Ministry would like to reiterate that it is taking the steps to strengthen privacy protection and ensure all staff are aware of their obligations when dealing with confidential, personal or sensitive information.

[53] As indicated earlier in this Report, I wrote to a number of police services and asked questions about their use of the Portal. In response, I received similar replies with respect to the communications and training that the police services received from the ministry. Police services confirmed that the training material provided used broad based searches as examples. They also explained that staff had concerns with the lack of results they were receiving when they were conducting searches. For this reason, users found it necessary to conduct searches using variations in the spelling of names and addresses, which resulted in multiple searches for a single call for service.

[54] I was also advised by several police services that although they were told to investigate the unauthorized broad based searches, when they contacted the ministry for

additional information to do this, it was not provided to them.

[55] Specifically, one police service advised the following:

> At your direction, a request was made to the Solicitor General's Office for the Audit Logs in relation to the dates and time of the 'potentially inappropriate queries' made by authorized members of the [a specific police service] to the Portal. The Solicitor General's Office, in e-mail correspondence to me on…has declined to provide any information citing concerns about perpetuating breach of privacy. Permission has been granted, by the Solicitor General's Office, to provide you with their specific response, as noted in their e-mail …

[56] The ministry's email response which is referred to above stated the following:

> My sincere apologies for the delayed response. With respect to your request, producing search results would involve accessing, using and disclosing personal health information (PHI) of individuals whose information was included in the Portal. The ministry is concerned that providing the search results from the searches conducted in the Portal could perpetuate potential privacy breaches and potentially create new ones. It is also not clear whether this access, use and disclosure of PHI is necessary as part of the IPC's investigation. Without this clarity of purpose and given the privacy concerns, the ministry is declining to provide the search results.
>
> I hope this information is of assistance to you.

[57] When I asked the ministry how providing the search results for the purposes of investigating a possible privacy breach would perpetuate potential privacy breaches, I received the following response:

> Some of the information that is now being requested from certain police services are the results that their authorized users would have received when they conducted specific queries in the Portal.
>
> Identifying which results would have been viewable by the authorized user when they conducted a municipality or postal code-wide search would effectively require re-conducting the searches to reproduce the results that would have appeared when the search was originally conducted. Producing these search results would involve accessing, using and disclosing the personal health information (PHI) of individuals whose information was included in the Portal. As such, the ministry is concerned that providing the search results from the searches in the Portal could perpetuate potential privacy breaches.

> The Ministry deleted the website and search tools that constituted the Portal when it shut the Portal down in July 2020. Re-conducting Portal searches would require reconstructing the Portal.
>
> Even if the Portal were to be reconstructed, it may not be possible to yield the search results that would have appeared when the search of interest was originally conducted. The dataset that was made searchable through the Portal was compiled cumulatively over time, so conducting a Portal search on the final dataset (i.e., as it existed when the Portal was shut down) would likely yield more results than conducting the same search on an earlier date while the Portal was operational.

[58] I do not accept the ministry's general assertion that providing the search results to the police to investigate a potential privacy breach that the ministry identified would perpetuate another breach. In the context of an investigation, an audit is a critical tool, the main purposes of which is to determine whether inappropriate access had occurred, what information was accessed inappropriately, the scope of the breach and who is affected. The response from the ministry raises concerns regarding the ministry's understanding of what is necessary to conduct a privacy breach investigation. It also demonstrates the absence of adequate support to police services who were being held responsible for investigating the privacy breaches and potentially notifying affected individuals.

[59] Regardless, as a practical matter, according to the ministry, it was unable to reproduce the search results because the Portal was shut down and the search tools were deleted along with the website. As a result of the above, many police services were unable to go further in their investigations.

[60] Accordingly, I find that the ministry's response to the privacy breach and the steps they took were not adequate in the circumstances.

[61] In coming to this conclusion, I have taken into consideration the fact that the ministry's response to the possibility that privacy breaches were occurring, was essentially to download to the police services the responsibility of investigating the breach and potentially notifying affected individuals, without providing them with the information they needed to do so.

[62] The implementation of the Portal was an extraordinary program that lasted only a few months, and in retrospect, was poorly communicated and executed from a privacy perspective. I trust that the ministry will carefully consider and implement the lessons learned from this experience in any new portal it considers creating in the future. In the circumstances, and given the discontinuance of the COVID Portal, I find it unnecessary to make any particular recommendations to the ministry beyond providing them with my findings and analysis in this report.

Summary of findings

1. The information at issue is "personal information" as defined by section 2(1)(b) and (h) of the *Act*.

2. The ministry did not have reasonable measures in place to prevent unauthorized access to the personal information in the Portal in accordance with section 4(1) of Regulation 460 of the *Act*.

3. The ministry's response to the breach was not adequate in the circumstances.

Other findings

[63] Despite the lack of detail provided by the ministry in relation to the audit, the police services I reached out to did provide me with explanations regarding their use of the Portal, and the steps they took to communicate to staff and address the matter of broad based searches and I am satisfied in that regard.

[64] With respect to the number of searches being conducted, the CCLA issued a press release on August 17, 2020 explaining that data it obtained from the Ministry of the Attorney General showed that, in the time the Portal was active, Ontario police had accessed the Portal over 95,000 times. The number of searches conducted by the OPP was noted to be 3,692 at the time the Portal was decommissioned. Without knowing the context, the volume of searches did appear to be very high and gave rise to an appearance that there was indiscriminate use of the Portal.

[65] As part of my investigation, I reviewed the number of Portal searches conducted by several police services, and compared them to the number of calls for service they received. The following information relates to the highest Portal searches:

Calls for Service	vs.	Searches conducted
46,379		24,623
12,383		14,831
104,570		13,551
24,462		10,475
34,433		10,293

[66] As previously indicated some users were conducting multiple searches in relation to each call for service. These searches included variations of names and addresses. In addition, I was advised that one call for service could involve more than one party, and as such, multiple searches would be conducted. After receiving these explanations and comparing the number of Portal searches relative to the number of calls for service, I do not find them so disproportionate as to necessitate this office to further investigate the matter at the level of each individual police service. My decision takes into account the fact that this matter was a unique situation in time, has already been publicly called out

and highly mediatized, and lessons have hopefully been learned. My decision also takes into consideration the practical fact that the Portal has been discontinued and the ministry has indicated it may not be possible to yield the search results that would have appeared when the search of interest was originally conducted.

Original Signed by: September 15, 2021

Lucy Costa
Manager of Investigations