Northwest Territories

Annual Report 2022 – 2023

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

If you would like this information in another official language, call us.
English

Si vous voulez ces informations dans une autre langue officielle, contactez-nous.
French

Kīspin ki nitawihtīn ē nīhīyawihk ōma ācimōwin, tipwāsinān.
Cree

Tłı̨chǫ yatı k'ǫ̀ǫ́ Dı wegodı newǫ dè, gots'o gonede.
Tłı̨chǫ

ʔerıhtł'ís Dëne Sųłıné yatı t'a huts'elkër xa beyáyatı theɔ́ą ɔat'e, nuwe ts'ën yółtı.
Chipewyan

Edı gondı dehgáh got'ı̨e zhatıé k'ǫ́ǫedatł'éh enahddhę nıde naxets'ę́ edahłí.
South Slavey

K'áhshó got'ı̨ne xədə k'é hederı ɔedı̨htl'é yerınıwę nídé dúle.
North Slavey

Jii gwandak izhii ginjìk vat'atr'ijąhch'uu zhit yinohthan jì', diits'àt ginohkhìi.
Gwich'in

Uvanittuaq ilitchurisukupku Inuvialuktun, ququaqluta.
Inuvialuktun

ᑖᒃᑯᐊ ᑎᑎᖅᑲᐃᑦ ᐱᕕᒐᔪᐊᕆᑦ ᐃᓄᒃᑎᑐᓪᓗᖅᓯᒪᓕᑎᒃ, ᐅᖃᖅᑎᖅᓄᑦ ᐅᖅᑲᓕᕐᓇᖅᑐᑎᑦ.
Inuktitut

Hapkua titiqqat pijumagupkit Inuinnaqtun, uvaptinnut hivajarlutit.
Inuinnaqtun

Office of the Information & Privacy Commissioner : (867) 669-0976
Commissariat à l'information et à la protection de la vie privée : 867-669-0976

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

July 1, 2023

The Honourable Frederick Blake
Speaker of the Legislative Assembly
PO Box 1320
Yellowknife, NT
X1A 2L9

Dear Mr. Speaker,

Pursuant to section 68 of the *Access to Information and Protection of Privacy Act* and section 173 of the *Health Information Act,* I have the honour to submit my Annual Report to the Legislative Assembly of the Northwest Territories for the period from April 1, 2022, to March 31, 2023.

Your truly,

Andrew E. Fox
Information and Privacy Commissioner
of the Northwest Territories

/af

Mailing Address: PO Box 382 Yellowknife NT X1A 2N3
Phone: (867) 669-0976 Toll-Free: (888) 521-7088 Email: admin@oipc-nt.ca

Table of Contents

Commissioner's Message

The past year has been busy and challenging. The number of new files decreased from the previous year, but many of last years' files remain open as they go through the review process. New privacy breaches filed under the *Health Information Act* decreased significantly. This may, at least in part, be due to better privacy protection measures being in place within health information custodians and public bodies. It may also be due in part to the dissolution of the COVID-19 Coordinating Secretariat, which reported a significant number of privacy breaches over its short existence. Inasmuch as most of the recommendations in review reports issued under the *Health Information Act* in the last few years have been accepted, it is reasonable to expect some reduction in the incidence of privacy breaches. It is perhaps a bit early to draw any firm conclusions, but there is room for optimism.

The number of files proceeding under the *Access to Information and Protection of Privacy Act* has also decreased. The number of complaints about delay has started to increase while the number of applications by public bodies for extensions of time have been decreasing. The Access and Privacy Office (APO) has been the designated Coordinator to receive and process access to information requests for all government departments and the NWT Housing Corporation since March 2021.[1] In July 2022, I learned that, in approximately half of all requests, the public bodies do not respond within the statutory time periods. As I discuss further below, the number of trained personnel in the APO is insufficient. This situation requires rectification.

The difficulty in providing timely, accurate responses to access to information requests is not unique to the Northwest Territories.[2] In my view, the public bodies need to allocate more resources for access to information activities: action is required, not complacence. Public

[1] So designated per section 68.1 of the Act.
[2] See news reporting at https://www.theglobeandmail.com/canada/article-secret-canada-investigation-backstory/

bodies undoubtedly have other policy priorities competing for resources, but complying with the *Access to Information and Protection of Privacy Act* is not a policy option: it is a legal obligation.

When complaints reach our office, we first determine whether some informal resolution is possible.[3] Not infrequently, a concern regarding the contents of a response to an access to information request, or to a possible breach of privacy, can be resolved through discussion and without the need for a formal review. Sometimes, individuals who are unfamiliar with the legislation simply need assistance to understand the legislation or how best to achieve their objectives. Wherever possible, and where appropriate, we attempt to facilitate early resolution.

On an operational note, our office is undergoing some changes in office space and in personnel. To accommodate staffing increases and the commensurate need for more appropriate office space, the Legislative Assembly recently agreed that a change in venue would be appropriate. The process for finding new space has begun and we expect to complete the move in the 2023-24 fiscal year and with minimal interruption in client service. In January of 2022 our new Investigator position was staffed; in late fall last year our Assistant Commissioner, Dylan Gray, announced he would be retiring early in the new year. Dylan's detailed, extensive knowledge of the *Health Information Act* and strong passion for protecting privacy made him a tremendous asset to the office. We wish Dylan all the best and thank him for his hard work and service.

[3] This is specifically contemplated in section 144 of the *Health Information Act*.

Financial Report

The total amount spent to operate the Office of the Information and Privacy Commissioner (OIPC) of the Northwest Territories for the fiscal year 2022/2023 was $ 736,202.84. A detailed breakdown is outlined in the charts on the next page.

The administration of the OIPC budget was again uneventful. This years total operating budget was $ 822,000.00 and we returned $ 85,797.16 to the Legislative Assembly. There were a few circumstances affecting variances between actual and budgeted amounts, and a few other notable circumstances affecting finances:

1. Funds returned to the GNWT were mostly from unused money budgeted for Travel to conferences and related expenses for hotels, transportation and per diems. As professional conferences have largely resumed as in-person events, we expect this budget line to be more fully utilized going forward.

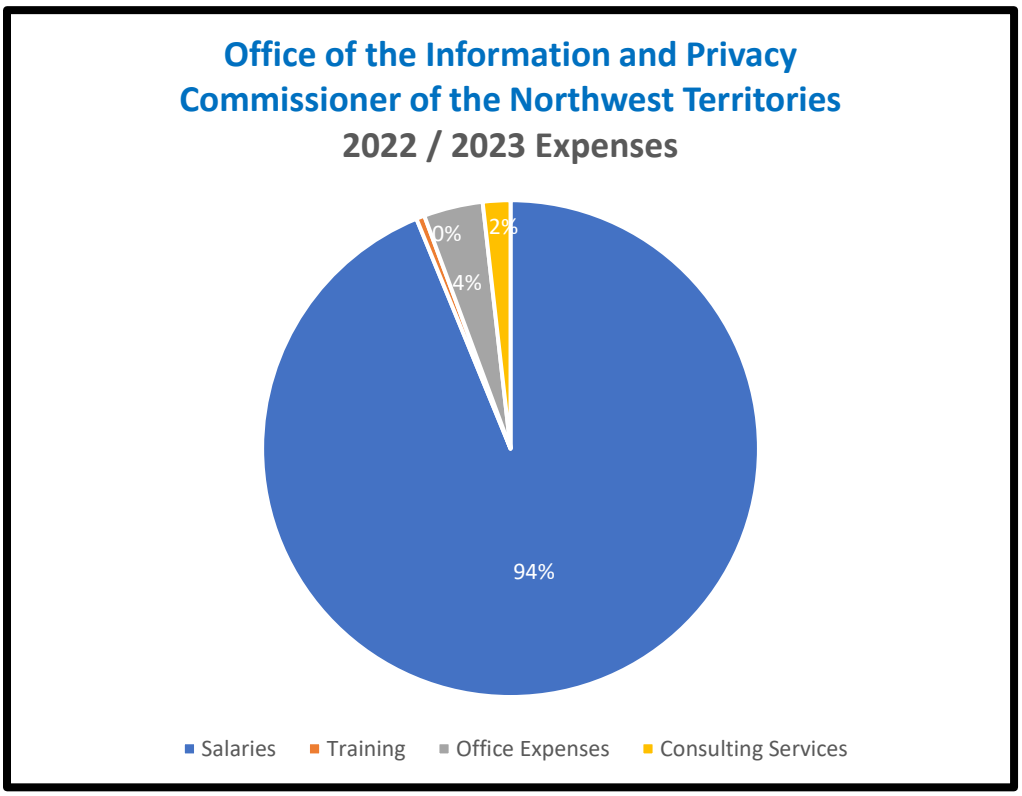
2. Professional development and training for staff is a continuing expense. Our Investigator and Assistant Commissioner were both enrolled in on-line courses through the University of Alberta.

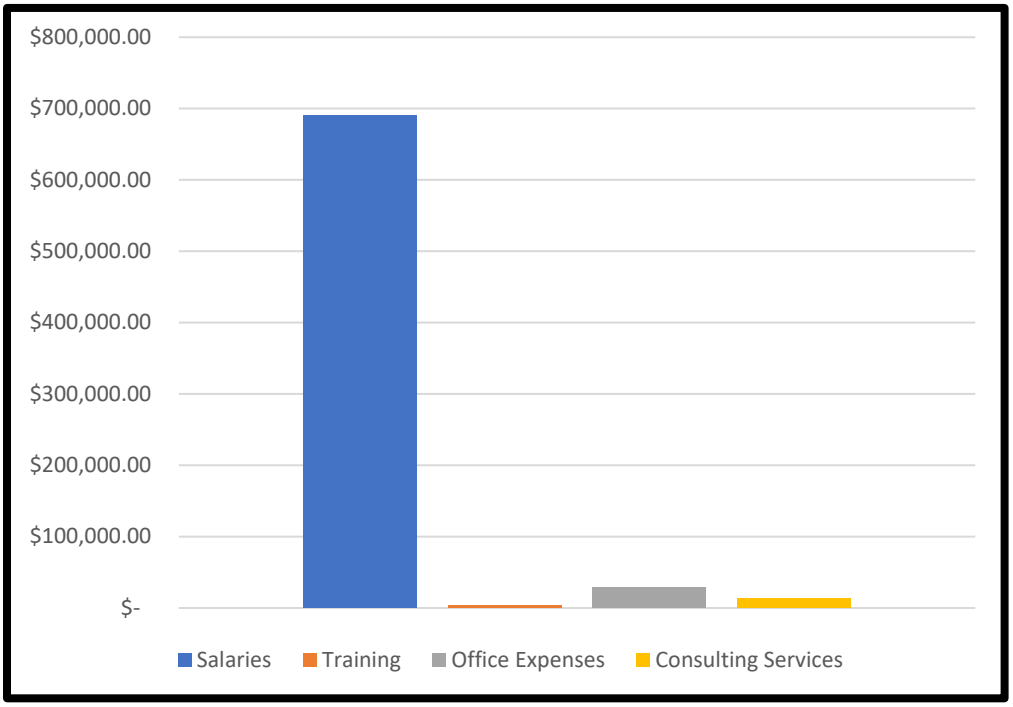
3. Our office continues to use the services of a consultant to assist with reviewing Privacy Impact Assessments. The number of new assessments submitted for review decreased this year and therefore we did not use all the allotted funds. This is a fluctuating source of work-demand, but with the new requirement for privacy impact assessments under the *Access to Information and Protection of Privacy Act*, we expect this to be a significant resource draw. We will be monitoring this activity closely.

4. All workstations received an upgrade to the office computer set up which has improved workflow and efficiency.

5. New office space is being arranged for this year, and we expect some additional expenses related to moving and fit-up requirements.

6. Our Assistant Commissioner/Investigator retired in 2023. We are engaged in the recruitment process to find a replacement for this position, and hope to have the position filled by the summer/fall of 2023.


Office of the Information and Privacy Commissioner of the Northwest Territories
2022 / 2023 Expenses
0%
4%
2%
94%
Salaries
Training
Office Expenses
Consulting Services


$800,000.00
$700,000.00
$600,000.00
$500,000.00
$400,000.00
$300,000.00
$200,000.00
$100,000.00
$-
Salaries
Training
Office Expenses
Consulting Services

Office of the Information and Privacy Commissioner and Enabling Legislation

The Access to Information and Protection of Privacy Act

The *Access to Information and Protection of Privacy Act*[4] *(ATIPPA),* applies to the departments, branches, and offices of the government of the Northwest Territories, plus 22 agencies, boards, commissions, corporations, and other public bodies designated in the regulations to the *Act*.[5] With the amendments that came into force in 2021, municipalities may be designated as public bodies by regulation.[6]

The *ATIPPA* enshrines four key rights and obligations:

- the right of the public to have access to records in the custody or control of a public body, subject to specific, limited exceptions;
- the right of individuals to have access to their own personal information held by public bodies and to request corrections to their own personal information;
- the obligation of public bodies to protect the privacy of individuals by preventing the unauthorized collection, use or disclosure of personal information; and
- the right to request independent review of public bodies' decisions regarding access to government records or regarding the collection, use, disclosure, or correction of personal information.

The *Act* has two fundamental purposes: to provide access for the public to government records and to provide protection for individuals' privacy by controlling the government's collection, use, and disclosure of personal information. Part 1 of the *Act* sets out the right of the public to access records held by public bodies and outlines a process for members of the public to obtain access to such records. Part 2 governs public bodies' collection, use, and disclosure of individuals' personal information. Amendments to the *Act* that came into force in 2021 provided additional privacy breach response requirements and introduced privacy impact assessment requirements.[7]

The Commissioner provides independent review of public bodies' decisions and actions under both Parts of the *Act*. After investigating the facts and receiving representations from the applicant or complainant, from the public body, and from any third parties, the Commissioner will issue a review report. A report may contain one or more orders or recommendations. A

[4] *SNWT 1994, c 20.*
[5] Subject to limitations and exceptions set under ATIPPA or other legislation.
[6] No communities have yet been designated.
[7] Substantial amendments were passed in SNWT 2019 c.8 and came into force on July 30, 2021.

public body is required to comply with a Commissioner's order, subject to appeal to the Supreme Court of the Northwest Territories.

Access to information and protection of privacy are both essential to ensure transparency and accountability of government -- vital elements for a healthy and effective democracy. Although access to government records is a legal right, it is not unfettered: there are statutory exceptions – some mandatory, some discretionary – that permit public bodies to withhold all or part of some records. Protecting the public's right of access to information and applying the relevant statutory exceptions can involve potentially complex decisions. Independent oversight helps to ensure public bodies apply the *Act* correctly, helping to assure applicants that their rights are being upheld.

The Health Information Act

The *Health Information Act*[8] (*HIA*) governs the collection, use and disclosure of personal health information. It codifies the right of individuals to access their personal health information, the obligation of health information custodians to safeguard individual privacy and ensures that personal health information is available to support the provision of health care services. The *HIA* regulates health information custodians in both the public and the private sectors, including the Department of Health and Social Services, the Northwest Territories Health and Social Services Authority, the Hay River Health and Social Services Authority, the Tłı̨chǫ Community Services Agency, and private physicians and pharmacists operating in the Northwest Territories.

The *HIA* requires health information custodians to take reasonable steps to protect the confidentiality and security of individuals' personal health information. It also gives patients the right to limit the collection, use and disclosure of their personal health information, and to put conditions on who has access to their personal health records and what personal health information may be accessed. Underlying these provisions is the principle that a health service provider's access to an individual's personal health information should be limited to the information the health service provider "needs to know" to do their job.

The *HIA* also requires health information custodians to notify affected individuals[9] if personal health information is used or disclosed other than as permitted by the *Act*, or if it is stolen, lost, altered, or improperly destroyed. Notice to the Commissioner is required in the event of an unauthorized disclosure, or in the event of unauthorized use, loss, or destruction where there is a reasonable risk of harm to an individual.[10] The Commissioner may initiate an investigation of a privacy breach upon the request of an individual who believes their personal health information was collected, used, or disclosed in contravention of the *Act*, or, in appropriate circumstances, the Commissioner may initiate a review independently. After conducting a review, the Commissioner will prepare a report and may make recommendations to the health information custodian. The health information custodian must notify the Commissioner of the health information custodian's decision to follow [or not to follow] the recommendation(s)

[8] SNWT 2014, c 2.
[9] Section 87 of the *Health Information Act*.
[10] Section 87 of the *Health Information Act* and Section 15(2) of the *Health Information Regulations.*

within 30 days of receiving a report. Further, the health information custodian must comply with a decision to follow the Commissioner's recommendation within 45 days of giving notice of the decision to the Commissioner. Applicants who are unsatisfied with a health information custodian's decision regarding a recommendation may appeal the decision to the Supreme Court.

The Information and Privacy Commissioner

The Information and Privacy Commissioner is a Statutory Officer of the Legislative Assembly of the Northwest Territories, appointed by the Legislative Assembly for a five-year term. The Commissioner operates independently of the government and reports directly to the Legislative Assembly.

The Commissioner's powers, duties and functions set out under the *Access to Information and Protection of Privacy Act* (*ATIPPA*) and the *Health Information Act* (*HIA*) are carried out through the Office of the Information and Privacy Commissioner (OIPC). The Commissioner's primary functions involve receiving and reviewing complaints about breaches of privacy and about the adequacy of public bodies' responses to access to information requests.

The Commissioner will also review and comment on Privacy Impact Assessments (PIAs) that are submitted to the Office of the Information and Privacy Commissioner. PIAs are generally required when a public body or health information custodian is developing a new system, project, program, or service involving the collection, use or disclosure of personal information or personal health information. PIAs are a key planning tool to ensure that the privacy implications of proposed policies or programs, etc., are considered at an early stage. A PIA helps identify where policies or programs align with legislative requirements and identify gaps or weaknesses that may require resolution *before* implementation. PIAs have been required under the *HIA* since it came into force in 2015, since 2019 under the GNWT's Protection of Privacy Policy 82.10, and since 2021 under the ATIPPA.

In addition to PIA's, the Commissioner may also review and comment on proposed legislation regarding possible implications for privacy protection or access to government information.

The Year in Review

The Office of the Information and Privacy Commissioner opened a total of 177 files in the fiscal year 2022/2023. Of these, 57 were matters within the scope of the *Access to Information and Protection of Privacy Act* and 120 are governed by the *Health Information Act*.

Overview of the Numbers

Access to Information and Protection of Privacy Act (ATIPPA)

The OIPC opened 57 files under the *Access to Information and Protection of Privacy Act* between April 1, 2022, and March 31, 2023:

Request for Review – Challenging redactions made in access response	4
Request for Review – Fees, Delays, Extensions or Refused access	8
Request for Review – A 3rd Party requests a review	1
Request for Review – Breach of Privacy complaint	7
Request for Review – Correction to records	1
Request for Time Extension for Public Body to respond to access request	19
Notification from Public Body - Breach of Privacy	12
Consultations/Comments – Acts, Legislations, Bills, PIA's	4
Miscellaneous and Administrative	1

Health Information Act (HIA)

The OIPC opened 120 files under the *Health Information Act* between April 1, 2022, and March 31, 2023:

Notifications from Public Body - Breach of Privacy	105
Request for Review – Privacy Issues and Complaints	2
Comments – Privacy Impact Assessment (PIA)	9
Comments – Health Policies, Acts, Processes	1
Miscellaneous and Administrative	1
Special Projects or OIPC initiated Reviews	2

Access to Information and Protection of Privacy Act

Section 68 of the *ATIPPA* requires the Annual Report to provide an assessment of the effectiveness of the *Act* and to report on the activities of the Commissioner and any instances where recommendations of the Commissioner were not followed. The following matters are relevant to these requirements, and I also include some separate recommendations for consideration by the Legislative Assembly.

Review Reports

Our office issued thirty-one review reports under the *Access to Information and Protection of Privacy Act* (*ATIPPA*) in 2022/2023. Twenty reports dealt with public bodies' applications for extensions of time to respond to access to information requests. Seven reports reviewed public bodies' responses to access to information requests. Four reports reviewed allegations that personal information had been collected, used, or disclosed without legal authorization.

Review reports are publicly available on-line at https://www.canlii.org/en/nt/ntipc/ .[11]

The Commissioner may issue orders at the conclusion of reviews. These orders are binding on public bodies. To monitor compliance, orders will direct the public body to report back to our office on its compliance activity. Thus far, we have not identified any compliance issues.

The Commissioner may still make formal recommendations for a public body's consideration when dealing with privacy breaches involving personal information.[12] If a privacy breach is "material"[13] the head of a public body must provide a report to the Commissioner about the breach of privacy. If the Commissioner determines the privacy breach creates a "real risk of significant harm" to one or more individuals, the Commissioner may recommend the head take steps to provide further notice, to limit the consequences of a breach, or to prevent further breaches of privacy. The head of a public body decides whether to follow any recommendation and reports to the Commissioner regarding the implementation of any accepted recommendations. My office did not receive a notice or report regarding a personal data breach under Division E this past year.

Time Extension Requests

My office received twenty extension-of-time requests from public bodies and issued nineteen extension Review Reports between April 1, 2022, and March 31, 2023. This is a relatively new category of review report. Prior to July 30, 2021, public bodies could extend the time to respond to an access request for a "reasonable period," subject to review by my office upon request.

[11] Past years' decisions are also available on-line on this free public database.
[12] Division E of Part 2 of *ATIPPA*
[13] The *Act* does not define this term but there are factors to consider set out in subsection 49.9(2).

Formal review reports for such situations were infrequent. If there was a complaint of a delay, a preliminary inquiry by the Commissioner would often lead to a resolution of the problem without need of a review.

Since July 30, 2021, the process for extending time periods has changed. Public bodies have an initial 20 business days to respond to an access to information request and can extend this period once for up to 20 business days if the conditions prescribed in section 11(1) are satisfied. Any further extension requires authorization by the Commissioner. An application for authorization must be submitted prior to expiration of the existing time period. If the time period expires first, the *Act* deems this a refusal to respond.[14]

Time extensions for third-party consultation

Fifteen Extension Review Reports addressed requests for time extensions to accommodate public bodies' consultation with third parties. Consultation is required where third-party personal information could be disclosed in a response to the access to information requests. Third-party consultation requires 55 business days to complete.[15] In every case this will exceed the 20 business-day extension available under subparagraph 11(1)(c), and therefore requires an extension authorization by the Commissioner under section 11.1.

In the normal course, where the public body requires a 55 business-day extension to conduct third-party consultation, there is no basis for the IPC to deny an authorization and the authorization process is essentially a 'rubber stamp'. In my view, this process warrants further consideration.

Recommendation 1: *The legislative assembly should consider amending the ATIPPA to allow a public body to extend the time once for the period required to complete third-party consultation without authorization by the IPC. For subsequent extensions, public bodies should continue to seek authorization from the IPC.*

Delay in responding to access to information requests

Subparagraph 11(1)(b) allows an extension of time for the public body to respond to an access request when a large number of records is requested or must be searched to identify the record requested, and meeting the time limit would unreasonably interfere with the operations of the public body. Prior to the 2021 amendment, a public body could rely on this provision to grant itself an extension of time of a "reasonable period" to respond to an access request, sometimes more than once. A public body may now only grant itself one extension of 20 business days and must seek authorization from the Commissioner for any further extension.

The Government of the Northwest Territories (GNWT) has created the Access and Privacy Office (APO) to provide support to all GNWT departments[16] to fulfill their *ATIPPA* obligations. Through this "Centralized Service Model" the GNWT has assigned many of the public bodies' access to information functions to the APO. This promotes and concentrates expertise within that office,

[14] See section 8(2) of the *Access to Information and Protection of Privacy Act*
[15] This includes a 40 business-day period to render a decision and a 15 business-day appeal period.
[16] And the Northwest Territories Housing Corporation

helping to bring critical knowledge and experience and efficiency to the access to information process.

Over the year, I received two requests from public bodies for a 20 business-day extension of time and three other requests for longer extensions to deal with large volumes of records. During this period there has been an increase in the number of complaints to our office of delay from applicants awaiting responses to their access to information requests. The APO says that when it is unable to respond to an access request in the time allowed it will often not seek an extension of time to respond but rather apply its limited time resources to the task of preparing the response on behalf of the public body. This is, in a sense, a pragmatic approach to dealing with the problem of having insufficient resources to provide a response within the time periods set by the *Act*: the task of applying for a time extension will slow response time further by drawing away limited resources from the task of providing the actual response. However, this approach confuses the public's reasonable expectations about process and response times, and it ignores the requirements of the legislation.

In July 2022, I accompanied a representative of the APO to a meeting with senior GNWT officials. The APO representative advised the group that responses to access requests were being provided late slightly more than 50% of the time. I do not believe the APO is solely responsible for the delays; I am advised that delay is sometimes exacerbated by the public body taking too long to review and approve a response. In my view, the Access and Privacy Office is a good administrative mechanism for the GNWT to provide access to information to the public. Having dedicated resources and trained, experienced staff is better than having access to information dealt with from 'the corner of the desk' of public bodies' employees who are already in full-time positions. However, without sufficient resources, this mechanism will not function properly, and it is apparent that the APO is not staffed sufficiently to adequately assist public bodies discharge their legal obligations in a timely way.

Legally, delays are the responsibility of the public bodies. Among the 2021 amendments were provisions that shortened the timelines for responses and created new authorization requirements for time extensions. The APO confirmed recently that its staffing level has not changed since 2022 and, not surprisingly, response times have not improved. It appears that public bodies are relying on the APO's assistance without ensuring the APO is sufficiently resourced and despite knowing that responses are being provided late at least half of the time. In such circumstances, relying on the APO to discharge legal obligations is not reasonable. It also appears to be out of step with the direction provided by the legislature, which is to decrease the waiting time between the submission of an access to information request and the receipt of the response.

The government has previously stated that "initial funding related to the implementation of a centralized ATIPP unit for the GNWT (the APO) was provided to the Department of Justice (DOJ) to ensure that there was consistency across government for the processing of access to information requests under the ATIPP Act, and also ensure that there was sufficient capacity and

expertise to process those requests efficiently and effectively."[17] This is a statement of intent; however, without sufficient resources, human and otherwise, the APO will not be able to adequately support the government departments to discharge their statutory obligations.

Recommendation 2: *The public bodies should review their legal obligations to respond to access to information requests and evaluate their capacity to provide responses within the legislated time periods. They should also ensure, either collectively or individually, that the APO is appropriately resourced so that it can reliably assist public bodies to respond to access to information requests within the legal time periods and to comply with the relevant procedural requirements.*

Reviews of Draft Legislation

Pursuant to section 67(1)(c) of the *ATIPPA*, the Information and Privacy Commissioner may provide comments on the implications for privacy protection arising from proposed legislation. The Department of Justice included this office in its public consultation process regarding proposed Missing Persons Legislation, and the Legislative Assembly provided the opportunity to comment on two other pieces of legislation. I trust that the comments were of some utility, and I look forward to reviewing future draft legislation.

Timelines in ATIPPA

Prior to the 2021 amendments to *ATIPPA* coming into force, the *Act* stated a review must be completed within 180 days of receipt of a request for review.[18] This period is now 90 business days.

While the OIPC supports the policy goal of providing an expeditious review process, adhering to a shortened deadline is difficult to achieve in practice. The average period to complete a review prior to 2021 was just over 12 months -- significantly more than 180 days. Our new Investigator came onboard in January 2022. That position was approved in 2020 based on increases to the file load that had already occurred. While OIPC staffing increased from three to four people (including the Commissioner), the number of files coming into the office doubled in the same period.

While my office will continue to work as thoroughly and efficiently as possible, it is unlikely that most reviews will be completed within 90 business days. While it may be useful for the Act to set a 'benchmark' timeline for completing a review, it would help clarify expectations of the review process if the Act expressly stated that the Commissioner could extend the period for completion of a review.

---

[17] See Government of the Northwest Territories Response to Committee Report 5-19(2): Report of the Information and Privacy Commissioner of the Northwest Territories at page 2. Located at: https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

[18] See section 31(3).

Recommendation 3: *The Legislative Assembly should consider amending the Access to Information and Protection of Privacy Act to expressly state the Information and Privacy Commissioner has discretion to extend the time required to complete a review. Such an amendment should include a requirement to give notice of an extension to all parties.*

Review Reports

Our office issued thirteen review reports under the *Health Information Act* this year. These reports, like those issued under the *Access to Information and Protection of Privacy Act*, are available on-line at https://www.canlii.org/en/nt/ntipc/.

Subparagraph 173(b) of the *Health Information Act* requires the Annual Report to report on recommendations that were made in a report to a health information custodian that were not accepted. This year, all recommendations were accepted by the health information custodians.

Alternative Resolutions

Privacy breaches may be addressed through a formal review when an individual requests a review or if the Commissioner determines this to be a useful approach.[19] Another approach is to work with the health information custodian to address a matter using alternate dispute resolution process [20] or, even less formally, by providing comment and guidance and identifying relevant resources for consideration. Alternative approaches are generally well received by custodians, and informal resolutions have led custodians to develop measures to prevent privacy breaches and to respond better to breaches when they occur. Where appropriate, I will continue to employ such alternative approaches to resolving privacy breaches.

Responding to Commissioner's Recommendations

At the conclusion of a review the Commissioner issues a report which may contain recommendations. After receiving a review report, a custodian has 30 days to decide whether to accept a recommendation and to notify the Commissioner of the decision.[21] The *Act* deems a failure to decide and notify the Commissioner of the decision within 30 days as a decision not to follow the Commissioner's recommendations.

Once a recommendation is accepted, the *Act* requires the custodian to comply with the recommendation within 45 days following that decision. However, there is no statutory oversight of a custodian's implementation of an accepted recommendation. Our office does not have any authority or resources to conduct such oversight, nor is there any legal obligation for a custodian to report on the implementation of any accepted recommendations. In comparison, the amended *ATIPPA* section 49.14 creates just such an obligation.[22] It would be helpful to have a required reporting process on the implementation of recommendations.

[19] On request by an individual under Section 134 or on the Commissioner's own initiative under section 137.
[20] Section 138.
[21] Section 156.
[22] 49.14. The head of a public body shall, within 120 business days of the notice given under paragraph 49.13(b), provide to the Information and Privacy Commissioner a report on the status of its implementation of recommendations accepted under section 49.13. SNWT 2019, c.8, s.34.

Recommendation 4: *The Department of Health and Social Services should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act, to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations.*

A Recommendation not accepted

The *Health Information Act* requires the annual report to identify any recommendations made in a review that are not accepted by a health information custodian. This year there was only one instance of this: in a review[23] dealing with a doctor taking the wrong prescription from a shared printer and giving it to the wrong patient, I recommended that NTHSSA install individual printers in examination rooms – the intent being to put the 'prescription pad' back into the privacy of the examination room. NTHSSA did not accept the recommendation, but indicated it was continuing "to explore technology and equipment improvements for its operations that balance privacy safeguards, infection prevention and control safeguards and operations.

In follow-up discussion with NTHSSA I learned that NTHSSA is pursuing the solution of individual printers in examination rooms. It agrees this is a good privacy safeguard and it is currently working on procuring the appropriate printers that meet regulations for health precautions. The decision to not accept the recommendation was based on the concern that putting a printer in all examination rooms is a significant practical obstacle in some existing health care facilities; however, I understand that examination rooms in new and planned facilities will be so equipped. The recommendation was not accepted in full, but neither was it rejected in full.

Incidence of Privacy Breaches

The number of new *Health Information Act* files decreased from 234 last year to 120 this year, and the number of privacy breach notifications from health information custodians decreased from 206 to 105. This is a significant improvement from the past year, though still approximately 30% higher than the year before that.

The following custodians reported breaches this year:

- Department of Health and Social Services (DHSS);
- Hay River Health and Social Services Authority (HRHSSA);
- Tlicho Community Services Agency (Tłı̨chǫ Community Services Agency);
- Northwest Territories Health and Social Services Authority (NTHSSA)

COVID Secretariat

Last year there were over 55 privacy breach notifications received from the COVID Secretariat. The Secretariat ceased operations in April 2022, and we received only one new privacy breach notice this fiscal year. Addressing these privacy breaches has been challenging. Many of the final breach reports were provided months after our office was notified, often missing pertinent

[23] Yellowknife Primary Care Centre (Re), 2023 NTIPC 23 (CanLII)

information, and answers to follow-up questions have often been provided months later. A frequent problem our office has encountered is the absence of records for some aspects of the Secretariat's operations: despite being a unit within the Department of Health and Social Services there were few or no records kept of the privacy training for personnel, although such records are required under the Department's *Mandatory Training Policy*. This is difficult to understand as the Secretariat was created as a unit within the Department[24] and the Department had relevant policies already developed to support compliance with the *Health Information Act*. The *Mandatory Training Policy* and the *Privacy Breach Policy* were created pursuant to a 2017 Ministerial Directive, and they bind all of the Department's employees. For reasons that remain unarticulated, the Secretariat did not act pursuant to these policies, nor does it appear that the Secretariat felt bound by them.

The Department advises that the Secretariat was, somehow, separate from the Department and that the Secretariat had not yet developed its own policies to address issues such as privacy training and privacy breach response. Why the Department's existing policies did not apply to the Secretariat is a conundrum. No real clarification or explanation has been offered beyond a general contention that the Secretariat was 'separate' from the Department. In my view this is a specious proposition and one which may have led to some confusion about privacy training requirements and proper privacy breach response. The Department had legal obligations as a health information custodian under the *HIA* and the policies that were promulgated to support compliance with the *HIA* apply to all parts of the Department.

In the government's report "Learning from the Response to COVID-19"[25] there is no discussion of the privacy breaches that occurred within the Secretariat, nor is there any discussion of the decision to situate the Secretariat within an existing health information custodian. There is no mention of the *Health Information Act* and the importance of protecting personal health information from unauthorized collection, use, or disclosure. Mistakes such as privacy breaches are perhaps inevitable when responding in a crisis, and I acknowledge that the many people who worked at the Secretariat performed valuable service to the residents of the Northwest Territories. However, the government should not forgo the opportunity now to take note of the legal and policy framework governing personal health information and take steps to prevent similar privacy breaches from occurring in any future pandemic.

Recommendation 5: *The GNWT should review the need for privacy-protective policies and procedures to support a specialized emergency response such as the COVID-19 Coordinating Secretariat and ensure it is equipped to operate within the bounds of the Health Information Act.*

NTHSSA

Most of the privacy breach notices were submitted by the Northwest Territories Health and Social Services Authority (NTHSSA), which provides health services to most communities in the Northwest Territories. The number of breach notifications is approximately half the previous

[24] https://www.gov.nt.ca/sites/flagship/files/documents/backgrounder_-_covid-19_coordinating_secretariat_final.pdf
[25] https://www.gov.nt.ca/en/newsroom/gnwt-releases-covid-19-lessons-learned-report

year's number,[26] but it is a 50% increase from 2 years ago.[27] The longer term trend is still increasing rates of privacy breach reports. Privacy breaches have frequently occurred while sending personal health information via fax[28], when sending emails, printing documents, and using electronic health information systems. Breaches have also occurred when documents have been lost on a public walkway[29] or when records have been accessed by employees for unauthorized reasons.[30]

NTHSSA has taken steps to improve awareness amongst staff about recognizing and responding to breaches, and its reporting process also seems to be improving. The number of privacy breach notices indicates there is more work to be done in applying the appropriate administrative, technical, and physical safeguards to protect personal health information. Despite the recurring nature of some types of privacy breaches, it does appear that the NTHSSA is striving to improve its ability to discharge its legal obligation to protect the confidentiality of the personal health information under its custody and control.

Recurring Issues in Privacy Breaches

Faxing

Though the circumstances may differ somewhat, the types of breaches reported are largely unchanged from previous years. Email continues to be an increasing source of privacy breaches, followed by misidentification of patients and their records and failure to apply reasonable security measures to paper records. Faxing remains a significant source of privacy breaches. There were 21 privacy breach notifications (20% of the breach notices) this fiscal year regarding faxing errors.

The incidence of unauthorized disclosure of personal health information when using fax machines has been addressed in past review reports and Annual Reports.[31] Faxing has also been the subject of comment by the Standing Committee on Government Operations.[32] The GNWT has previously advised it intends to reduce the use of faxing related to provision of health and social services over the last decade and that it "is preparing a plan to better understand the current use of faxing across the NWT HSS system and to continue the work toward further reducing faxing."[33]

---

[26] 206 Breach notifications
[27] 66 Breach Notifications
[28] Approximately 20% of the breach notifications were for faxing errors.
[29] *Northwest Territories Health and Social Services Authority (Re)*, 2022 NTIPC 19 (CanLII), https://canlii.ca/t/jtrzr
[30] *Northwest Territories Health and Social Services Authority (Re)*, 2022 NTIPC 13 (CanLII), https://canlii.ca/t/jt9r9
[31] For example, see 20-HIA 26 and 20-HIA 27 (CanLII) 2020 NTIPC 23 and 2020 NTIPC 24
https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc23/2020ntipc23.html
https://www.canlii.org/en/nt/ntipc/doc/2020/2020ntipc24/2020ntipc24.html
[32] https://www.ntassembly.ca/sites/assembly/files/cr_30-192_-_scogo_report_on_the_review_of_the_2020-2021_annual_report_of_the_information_and_privacy_commissio.pdf
[33] See Government of the Northwest Territories Response to Committee Report 5-19(2): Report of the Information and Privacy Commissioner of the Northwest Territories at page 3. Located at:
https://www.ntassembly.ca/sites/assembly/files/td_321-192.pdf

In 2022, the NTHSSA created a system-wide policy regarding faxing of patient information. This policy states "only information which is urgent for the continuity of patient care should be transmitted by fax." This is a useful restriction on the use of facsimile transmission; however, the same restriction appears in the predecessor policy document from 2011.[34] There are some differences between the two policy documents, and many similarities. Whether a new policy will have a significant effect on the incidence of privacy breaches remains to be seen.

The OIPC will continue to monitor this issue.

Recommendation 6: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information.*

Vigilance required when using email

The incidence of privacy breaches involving improper use of email has been increasing. Unauthorized disclosure can easily occur if an employee sends personal health information in an email to the wrong email address or to the wrong email group, or if they attach the wrong documents to an email. Emails that should have been messages to individuals have been mistakenly sent to large numbers of persons due to using "cc" instead of the "bcc" function. Inattention to detail is often the mistake that leads to such privacy breaches. The use of passwords on documents and secure file transfers can help reduce the possibility of an unintended recipient being able to access someone else's personal information when using email systems. These security measures are already specified to some degree in the *Electronically Stored and Transferred Information Policy*. As mentioned previously, proper privacy training is essential to ensuring that employees are aware of the applicable privacy protective measures.

Recommendation 7: *Health information custodians should utilize secure electronic transmission measures when transmitting personal health information.*

Privacy Training

Creating and maintaining a strong culture of privacy awareness and sensitivity to privacy protection issues is essential to reducing the number of privacy breaches that proceed from momentary inattention when handling personal health information. Training in privacy protective policies and procedures is essential to creating a privacy-protective workplace culture.

The Department of Health and Social Services (DHSS) created its *Mandatory Training Policy* in 2017, requiring privacy training for all employees of the Department, and the Health and Social Services Authorities. The Policy requires general and job-specific privacy training modules to be completed within three months of on-boarding new employees, and annually thereafter. It also requires the employer to keep a record of employees' training. The purpose of the *Mandatory Training Policy* is to ensure employees are trained to avoid or prevent privacy breaches before they occur and to respond appropriately in the event of a breach.

Employees acting in positions without appropriate privacy training, and management inadequately documenting training, continue to be issues. Custodians will often address training

[34] Stanton Territorial Health Authority's Facsimile Transmission of Patient Information policy dated January 2011.

deficiencies as part of their response to breach events, but this should not be necessary if custodians comply with the *Mandatory Training Policy*. Adequate employee training requires the dedication of resources and requires on-going support from leadership and management.

***Recommendation 8**: Health information custodians should prioritize implementation of, and compliance with, the Mandatory Training Policy and ensure that appropriate privacy training is provided for new employees, returning employees, and for all employees annually.*

Privacy Impact Assessments

This year our office reviewed and commented on nine Privacy Impact Assessments (PIAs) submitted by the DHSS and by the NTHSSA. Several of the PIAs addressed health information management and communications systems intended to support the government's response to the COVID pandemic.

The *HIA* requires a PIA to identify potential privacy risks posed by new health care information and communication systems, or changes thereto.[35] The Act also allows the Commissioner to comment on a PIA,[36] presumably so the custodian can reflect on those comments when finalizing design and implementation plans. Completing a PIA early in the planning phase of a project is better than later when other considerations (e.g., time or redesign costs) may make it difficult to make changes to improve privacy-protective safeguards. A PIA review should be completed well before project implementation, and certainly before any personal health information is subjected to the system and used operationally.

These are documents that take significant time to prepare, and reviewing a PIA also requires time – it is not a 'check-box' activity. Some PIAs have arrived in our office only days before the proposed project or system was scheduled to be implemented. Such timing suggests that the review of a PIA by this office is viewed more as a *pro forma* exercise at the conclusion of a project rather than an integral part of an early planning and design process.

PIAs are being submitted; however, more work needs to be done to utilize the PIA as part of project design. Unfortunately, the *HIA* does not address when a PIA is to be completed, or when it should be provided to the Commissioner, or even whether the Commissioner's comments need be considered. Practically speaking, however, a PIA should be completed and provided for review and comment at an early stage of project development so that any comments from the Commissioner can be considered and incorporated into project design where appropriate.[37] I note that amendments to the *ATIPPA* now expressly address these requirements for PIAs.[38]

[35] Section 89
[36] Section 175
[37] This is expressed in the GNWT's Protection of Privacy Policy 82.10. See subparagraph 6(3) at https://www.eia.gov.nt.ca/sites/eia/files/2019-09-19_protection_of_privacy_policy.pdf
[38] See section 42.1 of ATIPPA

***Recommendation 9**: Privacy Impact Assessments addressing any new information system or communication technology that involves the collection, use or disclosure of personal health information should be completed and submitted so that there is a reasonable period for review by the Information and Privacy Commissioner and for any comments to be considered by the health information custodian in the planning stages before implementation.*

***Recommendation 10**: The Legislative Assembly should consider amending section 89 of the Health Information Act to include similar provisions regarding privacy impact assessments as mandated in section 42.1 of the ATIPPA.*

Interjurisdictional Activity

The Federal, Provincial, and Territorial (FPT) Information and Privacy Commissioners continue to meet regularly online to share information, hear presentations, and discuss policies, technology, legislative proposals, and various other topics and issues pertaining to access to information and privacy protection. These meetings are a valuable forum to stay informed of policy developments at the national and international level.

The annual Information and Privacy Commissioners' conference was held in person in St. John's, NL in September 2022. In addition to receiving jurisdictional reports and several presentations on emerging issues, the conference finalized a resolution regarding the securing of public trust in digital health care. The resolution can be found at: https://priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_220921/ .

In November 2022, a second annual Investigators' Conference took place online. Both our office's Assistant Commissioner and Investigator participated in what was both a skill- based and knowledge-based learning event. By all accounts, it was a beneficial experience and our office will be attending again this year.

Final Thoughts

The right to privacy – the right to be let alone, to be free from intrusion or interference from others, including the state – is a fundamental right with a constitutional footing in section 8 of the *Canadian Charter of Rights and Freedoms*. The *Access to Information and Protection of Privacy Act* and the *Health Information Act* legislate specific privacy protections with respect to personal information held by our public government institutions.

When governments supply services to individuals, personal information is inevitably collected, used, and sometimes disclosed. As the digitalization of government services increases, electronic collection of personal information data – which is already significant – will continue to increase. Creating, using, and storing electronic data can create significant efficiency gains for governments in providing services to citizens. I am not alone in appreciating the convenience of renewing my driver's license and vehicle registration with the click of a few buttons rather than waiting in line at a registry office.

But, these gains are often accompanied by an increase in the risk of unauthorized use or disclosure. Personal information data sets can be the targets of bad actors engaged in ransomware or identity theft, and public governments are often the targets of such bad actors. Government must monitor the risk environment and protect those electronic systems containing personal information with reasonable security measures, i.e., privacy-protective system design, encryption, passwords, virtual private networks, secure file transfer protocols, user training, privacy-protective policies and procedures, regular auditing, and oversight, etc. Good privacy protection requires significant effort!

New threats are emerging. Many are raising concerns about 'Artificial Intelligence', both as a threat to privacy and as an existential threat. As the categories and sophistication of potential threats to privacy continue to grow, the effort and resources required to counter the threats must also grow. The government of the Northwest Territories has not suffered a major cyberattack, such as experienced by the government of Nunavut in 2019 or the government of Newfoundland's health care system in 2021, but the potential threat is clear and present. Every public body and health information custodian should be assessing its security measures and ensuring a strong defense to protect the personal information in their care and control.

It is fair to observe that extra layers of security can subtract from the potential efficiency gains. Sometimes, security measures such as passwords can be viewed as obstacles to efficiency; that is, until a privacy breach occurs. In a review completed this year,[39] I learned that a public body had stored a significant number of employee files in the digital integrated information management system (DIIMS) without password protection or other appropriate security controls. The files were exposed to unauthorized access by unauthorized employees, and this unfettered access had been going on for an extended period. The public body's response involved significant and costly efforts: several employees dedicated months of their time to dealing with the breach. This breach is an instructive example for public bodies to consider when deciding on

[39] *Applicant A (Re),* 2022 NTIPC 20 (CanLII), https://canlii.ca/t/jtpkw

the resources to devote to privacy-protective security measures: the cost implications, in both financial and human resources, of a privacy breach event can be very significant!

Going forward, I highly recommend that public bodies attend closely to the need for reasonable, effective security measures to protect the personal information entrusted to their care and control. Constant vigilance is essential.

Lastly, it is with great sadness that we note the passing of Ms. Elaine Keenan Bengts on August 8, 2022. After a long legal career which included serving the Northwest Territories and Nunavut as the first Information and Privacy Commissioner from 1997 to 2020, Ms. Keenan Bengts' plans for a well-deserved retirement were cut short by illness. Ms. Keenan Bengts had an inspiring, tireless passion for the work of this office and contributed much to the people of the Northwest Territories. She will be missed.

Summary of Recommendations

Recommendation 1: *The legislative assembly should consider amending the ATIPPA to allow a public body to extend the time once for the period required to complete third-party consultation without authorization by the IPC. For subsequent extensions, public bodies should continue to seek authorization from the IPC. (Page 10)*

Recommendation 2: *The public bodies should review their legal obligations to respond to access to information requests and evaluate their capacity to provide responses within the legislated time periods. They should also ensure, either collectively or individually, that the APO is appropriately resourced so that it can reliably assist public bodies to respond to access to information requests within the legal time periods and to comply with the relevant procedural requirements. (Page 12)*

Recommendation 3*: The Legislative Assembly should consider amending the Access to Information and Protection of Privacy Act to expressly state the Information and Privacy Commissioner has discretion to extend the time required to complete a review. Such an amendment should include a requirement to give notice of an extension to all parties. (Page 13)*

Recommendation 4*: The Department of Health and Social Services should consider implementing a policy, or the Legislative Assembly should consider amending the Health Information Act, to require health information custodians to report to the Commissioner regarding the implementation of accepted recommendations. (Page 15)*

Recommendation 5: *The GNWT should review the need for privacy-protective policies and procedures to support a specialized emergency response such as the COVID-19 Coordinating Secretariat and ensure it is equipped to operate within the bounds of the Health Information Act. (Page 16)*

Recommendation 6: *Health information custodians should continue to reduce or eliminate the use of fax machines to transmit personal health information. (Page 18)*

Recommendation 7: *Health information custodians should utilize secure electronic transmission measures when transmitting personal health information. (Page 18)*

Recommendation 8*: Health information custodians should prioritize implementation of, and compliance with, the Mandatory Training Policy and ensure that appropriate privacy training is provided for new employees, returning employees, and for all employees annually. (Page 19)*

Recommendation 9*: Privacy Impact Assessments addressing any new information system or communication technology that involves the collection, use or disclosure of personal health information should be completed and submitted so that there is a reasonable period for review by the Information and Privacy Commissioner and for any comments to be considered by the health information custodian in the planning stages before implementation. (Page 20)*

Recommendation 10*: The Legislative Assembly should consider amending section 89 of the Health Information Act to include similar provisions regarding privacy impact assessments as mandated in section 42.1 of the ATIPPA. (Page 20)*

Contact Us

Office of the Information and Privacy Commissioner
of the Northwest Territories
PO BOX 382
Yellowknife, NT X1A 2N3

Phone Number: 1 (867) 669-0976
Toll Free Line: 1 (888) 521-7088
Fax Number: 1 (867) 920-2511

Email: admin@oipc-nt.ca

Website: www.oipc-nt.ca

Our office is located on the first floor of the Laing building in Yellowknife
Corner of Franklin Avenue & 49th Street, the entrance is on Franklin Avenue