

2013

Annual Report

Office of the Access to Information and
Privacy Commissioner

Province of New Brunswick



July 2015

The Honourable Chris Collins
Speaker of the Legislative Assembly
Legislative Building
706 Queen Street
Fredericton, New Brunswick
E3B 1C5

Dear Mr. Speaker,

Pursuant to section 63 of the *Right to Information and Protection of Privacy Act* and section 64 of the *Personal Health Information Privacy and Access Act*, I submit our third Annual Report, that reports on the activities of the Office of the Access to Information and Privacy Commissioner for the fiscal year of operations from April 1, 2012 to March 31, 2013. Thank you.

Respectfully submitted,

Anne E. Bertrand, Q.C.
Access to Information and Privacy Commissioner
/

CONTENTS

FROM THE COMMISSIONER 2

PUBLIC OUTREACH AND AWARENESS 7

MANAGEMENT OF FILES 11

***Right to Information and Protection of Privacy Act* 13**

Breakdown of files handled under the Act in 2012-2013 14

 Informal Resolution Process 15

 Two and a Half Years of Access Complaint Outcomes 16

 Complex Investigations 17

 Issues Raised During Investigations 18

 Duty to Assist and Meaningful Responses 20

 Privacy Breach Notifications 21

 Privacy Concerns 21

 Types of Privacy Concern Outcomes 22

***Personal Health Information Privacy and Access Act* 23**

Breakdown of files handled under the Act in 2012-2013 23

 Privacy Breach Notifications 24

 Privacy Complaints 25

 Types of Privacy Complaints 26

Snooping cases 26

General Inquiries 27

WHO COMPRISED THE TEAM FROM APRIL 2012 TO MARCH 2013? 30

FINANCIAL INFORMATION 30

***Contact information* 30**

FROM THE COMMISSIONER

After more than two years, the goals we have set for ourselves are producing results. At the outset in September 2010, we felt it was more important to the long term and continued success of the implementation of the new statutes, *Right to Information and Protection of Privacy Act* and *Personal Health Information Privacy and Access Act*, for us to offer guidance for those who were and about to be subject to this legislation. We saw our role as one that was much more than purely that of a regulatory body. By the end of March 2013, our vision has remained: powers provided under both statutes permit the Commissioner and her Office to provide guidance and, over time, we used these powers as an effective means to promote the true spirit of the legislation and see to its successful implementation, while keeping a respectable distance to maintain impartiality in our investigations.

Our ability to provide “guidance” directed our oversight approach to be contemporary, educative, and, in our view, more effective. We encouraged a public sector shift surrounding the handling of regulation while focusing heavily on educating the health care sector which, for the most part, had not had experience in codified rules for the handling of personal health information. This was accomplished by demonstrating that there are benefits, and positive outcomes, to compliance. Positive outcomes manifest in various forms; for instance, those who seek information are very pleased with the access they obtain, and they also gain a better understanding of why some information cannot be lawfully released. Some who submit complaints do not completely understand our oversight role; they may be seeking findings of wrongdoing in order to collect financial compensation, or in the hopes of getting someone fired. A positive outcome from this is our ability to write decisions and rulings on how the legislation works, the obligations of those who hold the information, and how access complaints and privacy breaches can be concluded, resolved, and corrected without embarrassment or blame, and lessons learned to be applied in the future.

Public entities and health care providers alike gave us the benefit of the doubt and worked in cooperation to adopt access to information and protection of privacy principles in their organization. They thanked us for our thoroughness, good guidance, and feedback; they accepted our written comments and used them as helpful resources and acknowledged the positive outcomes that resulted from their participation. Evidence of this was observed through public entities reporting privacy breach incidents to our Office to obtain our guidance even where there was no obligation to do so under the law. Moreover, some organizations not

subject to the legislation asked for our oversight review to ensure they were handling access requests and protecting sensitive information lawfully.

Our experience has shown that the private health care sector remains reluctant in accepting that *Personal Health Information Privacy and Access Act* is law and that this statute is changing how they treat the private information of their clients or patients. In fact, many were not aware that these rules were meant to codify the standards surrounding privacy that they already know. The public is more aware of the statute and wants their health care professionals to provide answers when their most private information has been compromised, although prepared to be forgiving to regain the essential trust relationship that must exist with their health care professionals. We focussed on containing incidents of privacy breach, ensured that notification to those affected was carried out, and more importantly, ensuring that the standards of keeping patient/client information confidential be well understood and adapted in the workplace, with corrective measures to avoid future similar cases. We remained steadfast in our follow-up procedures to see that our recommendations are followed and implemented, in order to monitor compliance. Again: when we convey the positive outcomes that are derived from compliance, we see that the reluctance begins to disappear.

New Brunswick was the first province to have mandatory breach notifications for the healthcare sector under *Personal Health Information Privacy and Access Act*, while it is not mandatory for public bodies to notify us of privacy breaches under *Right to Information and Protection of Privacy Act*. Interestingly enough, while there are many more breach notifications in the healthcare sector, we have noted less interest due to a tendency to excuse those errors over the need for the public to obtain access to health care services. One exception to that rule remains, however, that the public will not excuse *snooping* in health care records.

Our public awareness campaign continued in full force this past year, with an increasing number of requests from public and private groups for us to give presentations in relation to the two statutes. This resulted in 21 lectures and presentations to groups from all sectors in this past year alone. These public engagement lectures and seminars are giving us opportunities to promote all of the positive aspects of the legislation, while providing guidance on how best to apply the rules – as challenging as they may sometimes be.

We reached out to the greater public during **Right to Know Week**, in order to make New Brunswickers aware of their right to know about access and privacy. During that week, we gave two presentations to municipalities, one in English and one in French, as municipalities became subject to *Right to Information and Protection of Privacy Act* in late 2012. We also participated in another public awareness campaign: **Data Privacy Day** held on January 28th 2013 and we took that opportunity to reach out to New Brunswickers, universities, and school districts in order to educate them on proper privacy safeguards.

In 2012-2013, we received in excess of 500 files of all types and description, meaning that since September of 2010, we have dealt with more than 1300 cases. This work translates into a solid base of experience and training for my staff and me. With the amount and variety of matters to handle over this period, we looked to 2014 to measure the work undertaken to determine, more importantly, whether we are getting tangible and effective results. We do this by tracking the recommendations that we issue in order to determine if the recommended changes to policies and practices will result in real progress for the Province and for the implementation of concrete practices that could mitigate future issues before they even occur. We want to determine whether or not our oversight function and our approach are creating real change.

From the workload undertaken, we are able to see trends and draw observations on a variety of fronts; one such observation is in the area of how public bodies process access to information requests. Overall, we have found that most public bodies are meeting their duty by first seeking clarification of the information requested which results in more thorough searches of records before responding. We have also found that public bodies are generally more inclined to assist those who make requests, and more apt to list all the records that are applicable while also explaining why access to some information is being refused. This results, again, in more meaningful explanations, all of which we believe reflects well on government and a population that is more informed, more aware. Going forward, we are encouraging public bodies to provide lists of records in order to make responses more meaningful and to ensure the applicant fully understands why some access to information is being refused. Meaningful responses, in turn, make those who request the information understand and less likely to complain.

As we are still a relatively new and developing oversight body, public awareness and education remained a priority. We have found that two of the most major concepts “privacy” and “consent” are widely referred to and relied upon but not always fully understood. In our guidance role, we strived to ensure that all those involved are clear on both concepts as they go about their activities. In terms of privacy, it seems as though the public is aware of its rights but not necessarily how to enforce them or of the role and powers of our Office as oversight body. As for consent, we found that an overreliance on complicated consent forms, as well as implied consent, led many to not be fully aware what they were consenting to or how their personal information was being shared.

During the past 2012-2013 year, the media played a more pronounced role in reaching the public and how the public perceives the issues we deal with; we noted a considerable increase in the amount of media coverage regarding access to information and privacy. We believe this is due, in part, to the fact that access to information and privacy are increasingly present in our

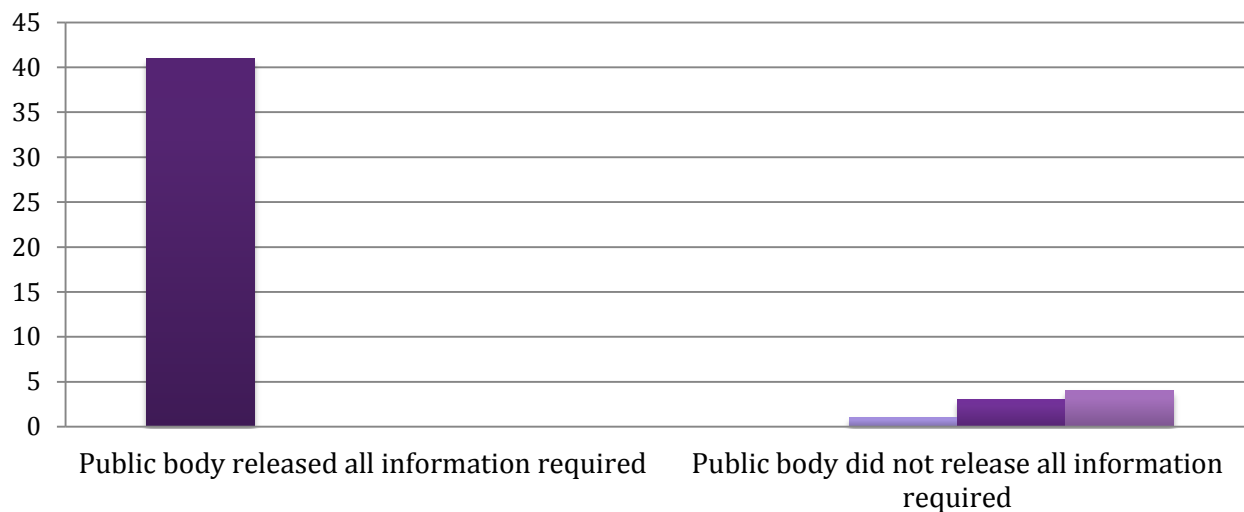
society, and in other parts of the world, and evidenced by the number of times I was asked to provide comments and observations on those subjects.

One major concern over information sharing and implied consent that occurred in the 2012-2013 period involved the War Amps key tag program. The issue arose when members of the public raised concerns over receiving mail from the War Amps key tag program, unaware that their personal information had been given out. The War Amps had gathered it from the drivers' licence database from an established practice within the Province after having been provided a list of all registered drivers from the database maintained by the Department of Public Safety, but without notice to holders of driver's licenses. Following our investigation, the Department followed our recommendation that future agreements with War Amps included safeguards to protect personal information, with adequate notice to drivers and an opting-out option for those who did not want to participate in the program. This case was one of many in our approach to investigate matters with a view to effect a good outcome, satisfactory to both the public and public bodies, and more importantly, in conformity with the legislation.

In similar fashion, our continued work to effect informal resolutions of complaints arising from non-satisfactory experiences in accessing information held by government resulted in a high rate of success.

Our informal resolution process is neither a mediated outcome nor one based in compromise; it is simply a satisfactory result founded in conformity with the legislation, where public bodies honour their statutory obligations and the public receives the information to which it is entitled under the law. We believe this approach to investigations exemplifies the service that the public rightfully deserves: a public sector more willing to accept the tangible benefits that come from disclosing information regarding its affairs and decisions made, and a public that is equally accepting of the information, good or bad, in order to be informed of government's business.

From September 2010 to March 31, 2013, we investigated and concluded 49 complaints of which 41 resulted in the required information being released. In only 8 cases was it necessary to issue formal recommendations. In other words, more than 4 out of every 5 cases concluded without formal recommendations, which meant that the public bodies agreed to disclose all of the information that ought to have been released at the outset. The graph below demonstrates how we track this progress, a progress that encourages us to continue with this approach.



- Public Body agreed & released information to resolve complaint - 41 cases
- Public Body issued formal recommendation - followed - 1 case
- Public Body issued formal recommendation - followed in part - 3 cases
- Public Body issued formal recommendations - refused - 4 cases

(September 2010 to March 31, 2013 access to information complaints outcomes)

It goes without saying that in 2.5 years at the end of March 2013, and with over 1300 cases, as an Office, we continued to grow, learn, and improve.

We continue to transfer the experiences acquired to those outside and aid public bodies in maintaining a high level of integrity in access to information and privacy, as well as ensuring that New Brunswickers know the full extent of their rights.

While recognizing there is always room for improvement, we discern what is working well and adjust that which is not in a relentless effort to continue firmly with our goal: promoting openness and transparency in our Province to ensure rights of access to information and protection of privacy are respected and maintained at all times.

Anne E. Bertrand, Q.C.

PUBLIC OUTREACH AND AWARENESS

Logo

Among other duties, the Commissioner has the mandate to inform and educate the public about the *Acts*. As a new office, tools to promote awareness of both pieces of legislation were still in their early stages and it became essential that this Office presented itself online. This platform allowed our resources to be readily available to a larger audience including those subject to the two statutes. An important aspect of our online presence was a logo that accurately represented the **balance between access to information and the protection of privacy**.

In the summer of 2012, the Commissioner's Office developed a logo that illustrates the balance between the key aspects of the two pieces of legislation: transparency and privacy.



The vibrant colours were selected for a modern and clean look, while the binary code signifies the future that this new legislation stands for. The binary code is visible through the file folder as a **sign of transparency** and the positioning of the folder clearly represents openness.

The keyhole on the outside of the folder stands for privacy as it indicates that there is also **data that must be protected**. With this logo the Office is now recognizable by the general public and this in turn helps the Commissioner in her mandate to raise awareness and inform New Brunswickers of their rights under the two statutes.

www.info-priv-nb.ca

On September 28, 2012, the Commissioner's Office launched its website. This website was developed with a **user-friendly approach** in mind not only for the general public but also for the public bodies and custodians who are subject to the *Acts*. Internal discussions lead to an understanding of the frequently asked questions at an intake level which were then developed and published for each of the respective *Acts*. With a **view to educate and serve** the public and those subject to the *Acts*, information and resources were also made available. As we continue to update the website with relevant and helpful information, we are also continuing to make New Brunswickers **aware of their rights** under both statutes, and we are dedicated to a website that is user-friendly and relevant to everyone: the general public and public bodies and custodians subject to the *Acts*.

Right to Know Week 2012: **September 24-28**
Right to Know Day: **September 28**

Among other mandates, the Commissioner is to inform the public about the Acts and, while she provides presentations all year around, Right to Know Week offers **an ideal opportunity to reach out to New Brunswickers** and make them aware of their Right to Know. In that regard, along with the launch of our website on September 28, 2012, we created Factsheets (also available on our website) that explain not only the process of requesting information but also what the two pieces of legislation mean and to whom they apply. These resources were distributed by employees of this Office and the Commissioner at the Regent Mall in Fredericton during Right to Know Week.



Photo: Employee talking to member of the public at the Regent Mall in Fredericton during Right to Know Week.

Right to Know Week celebrates the right of an individual's access to information held by public bodies and marks the benefits of transparent and accessible government.

Right to Know Day is celebrated around the world in over 60 countries that have access to information legislation.

As municipalities became subject to the *Right to Information and Protection of Privacy Act* on September 1, 2012, the Commissioner presented at two workshops, one in each official language, to municipalities during Right to Know Week.

Data Privacy Day – January 28, 2013

On January 28, 2013, Canada, along with many countries around the world, celebrated Data Privacy Day. This day recognizes **the impact of technology on our right to privacy** and is meant to **promote proper privacy safeguards** among companies, government officials, educators, and the general public. Canada’s theme for this year, which was developed by the Office of the Privacy Commissioner of Canada, was: **Take control of your information. Don’t let it come back to haunt you!**

The Commissioner gave two public lectures: one at St. Thomas University in Fredericton on January 28, 2013 and the other at the Edmundston Campus of the Université de Moncton on January 31, 2013 where she spoke about the implications of data privacy in New Brunswick.

We also took the opportunity to contact schools and school districts, which just became subject to the *Right to Information and Protection of Privacy Act* on October 1, 2012, by sending them posters published by our federal counterpart, the Office of the Privacy Commissioner of Canada as well as resources developed by our Office.

*“It is becoming increasingly important for New Brunswickers to pay attention to their personal information given the prolific use of social media in their daily lives. Data Privacy Day provides a great opportunity to **learn more about the importance of privacy** while also reminding those whose responsibility it is to protect personal information to do so at all times.” – Commissioner Bertrand*

Bookmarks

In light of Data Privacy Day and the Right to Know Week, we developed bookmarks. These bookmarks have been quite popular and are a simple way to provide our contact information to those who are interested in learning more about the two important statutes we oversee.



We developed bookmarks with **facts about New Brunswickers’ Right to Know**, and a second type that is geared towards privacy with the following helpful tips: **Think before you speak, Consider before you write and Pause before you click.**

We continue to hand these bookmarks out to the general public, public bodies and custodians. To date we have handed out over 6500 bookmarks and receive overwhelmingly positive feedback regarding the simplicity of the idea and the helpful tips.

PUBLIC EDUCATION

The Commissioner is asked to speak on various topics relating to the legislation we oversee and the work we do, and we strive to accept as many invitations as we can. Over the past year, we presented **to more than 20 various groups** during conferences, seminars, training sessions, workshops and board meetings for different organizations. Specifically, we addressed professional organizations, municipal officials, access to information and privacy professionals, researchers, law and journalism students, as well as private, public and not-for-profit organizations.

Municipalities became subject to the *Right to Information and Protection of Privacy Act* in September 2012. In that regard, we presented to municipal officials through a presentation to the municipal council of the City of Fredericton in October 2012. In addition, the Commissioner was asked to be a keynote speaker at the comprehensive training sessions for municipal officials at the Memramcook Institute. The training sessions focused on raising awareness of the legislation, providing guidance on how the rules should be applied and an overview of the complaint process.

Media

Over the past year, there has been a considerable increase in the amount of media coverage regarding access to information and privacy. For instance, files involving privacy breaches in both the health and public sector, and reports of the Commissioner have generated considerable interest from the media as **access to information and privacy considerations are increasingly present in our society**. This past year, the media has reported with great interest on issues related in some fashion to access and/or privacy on a regular monthly basis.

The Commissioner took the opportunity to address the media on several occasions in order to provide timely comments and observations with respect to areas of public interest.



*The Commissioner giving a public lecture at St. Thomas University
Photo: Julia Whalen/the New Brunswick Beacon*

MANAGEMENT OF FILES

Total Files

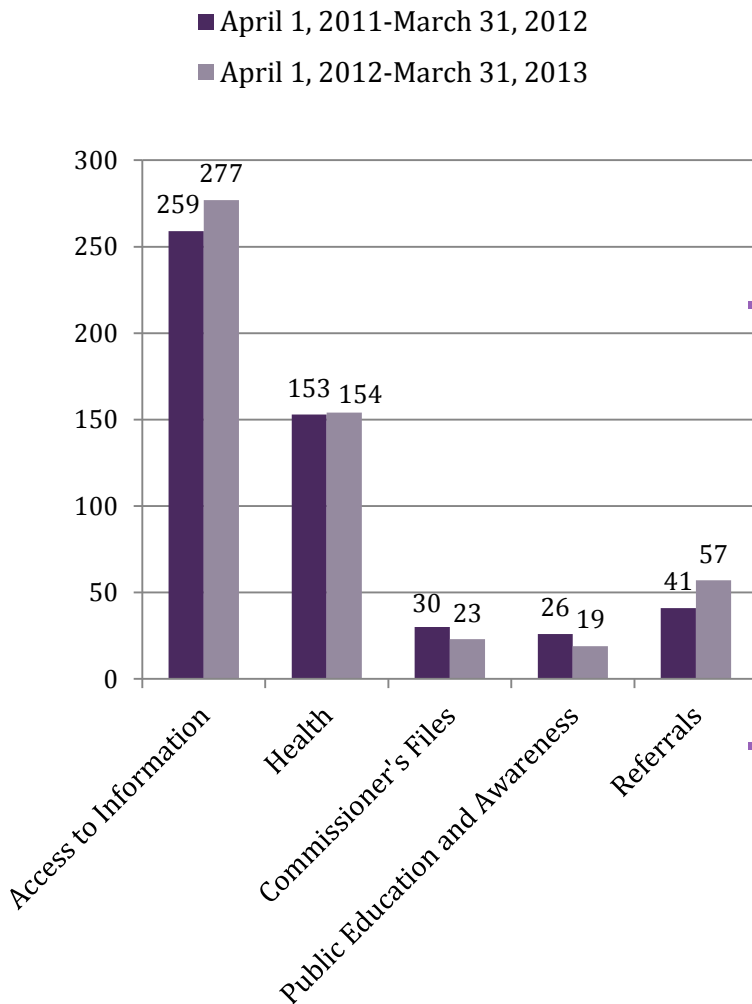
The graph below indicates the workload of our Office, as we were only able to conclude (close) 31 fewer files than the previous year.

The total number of files opened and carried over from 2012-2013 were more than those carried over in the previous year, illustrating how the Office has grown and continues to do so.



Types of Files Opened

We saw a rise this year in the number of Referrals and files opened under the *Right to Information and Protection of Privacy Act* compared to last year. Approximately the same number of Public Awareness files and files under the *Personal Health Information Privacy and Access Act* were opened as last year, and there were less Public Education and Commissioner’s Files opened. The full breakdown can be seen in the graph below.



Referral Files: *cases where individuals or organizations seek assistance for a particular matter that does not form part of our mandate. With a view to be helpful, we find the proper office before redirecting the case. We dealt with 57 referral files this year.*

Public Awareness Files: *opened when our Office carries out a specific project to raise awareness of the law or a particular aspect of the law. There were two such cases this year: Right to Know Week and Data Privacy Day.*

Public Education Files: *opened when the Commissioner gives a presentation about the legislation she oversees to those subject to the legislation. We opened 17 of these files this year that meant 21 presentations in total, in various parts of the Province.*

Commissioner’s Files: *opened by the Commissioner with the intent to investigate systematic issues surrounding either statute, or with the intent of provide useful resources to public bodies and health care providers. We opened 23 Commissioner’s Files this year.*

Right to Information and Protection of Privacy Act

The ***Right to Information and Protection of Privacy Act*** sets out rules for government departments, municipalities, universities, schools, and other **public bodies** for responding to requests for information, and for the handling and protection of **personal information**.

The Commissioner's mandate under the *Act* includes many different areas of responsibility:

- **Access Complaints** are filed by individuals or organizations who are not satisfied with the outcome of an access request.
- **General Inquiries** are questions we receive from individuals, organizations, media, and various other groups about the legislation.
- **Privacy Concerns** are filed by those who believe that a privacy breach has taken place, or that a public body's policy or practice may be in contravention of the legislation.
- **Privacy Breach Notifications** are opened when we are alerted by those subject to the legislation that a breach of privacy has occurred within their organizations.
- **Comments on Proposed Legislation or Programs** are opened when the Commissioner is asked to provide input on new legislation or programs that are being considered and that may impact access to information or the protection of privacy.
- **Time Extensions** are applications submitted by public bodies asking the commissioner to grant them more time to reply to an access request.
- **Requests to Disregard** are applications submitted by public bodies asking the Commissioner to permit them to disregard an access request in specific circumstances.
- **Late Complaint Extensions** are opened when an applicant files a complaint after the deadline to do so, and the Commissioner must examine whether she can exercise her discretion to accept a late complaint.
- **Media Inquiries and Interviews** are opened whenever the media asks our Office to comment on a privacy or access to information matter that is of interest to the public and being reported on in the news.
- **Public Advisories** are opened when we are notified of a matter that impacts the privacy of New Brunswickers but that does not fall under our mandate, and we assist in informing the public about the matter.
- **Best Practices** are issued to promote a better understanding of the rules of the legislation and to guide those who have to apply them.
- **Interpretation Bulletins** are issued to address questions that arise regarding the interpretation of the rules of the legislation and to guide those who have to apply them.

Breakdown of files handled under the Act in 2012-2013

Between April 1-2012 and March 31-2013, we opened **278 new files** under the ***Right to Information and Protection of Privacy Act*** while continuing our work on those carried over from the previous year. The following table shows a breakdown of the work on these files:

	Files Carried Over from Previous Year	Files Opened 2012-2013	Files Closed 2012-2013	Files Remaining Open at Year End
Access Complaints	16	55	29	42
General Inquiries	10	142	132	20
Privacy Concerns	9	11	15	5
Privacy Breach Notifications	2	9	5	6
Comments on Proposed Legislation or Program	2	4	4	2
Time Extensions	0	10	9	1
Requests to Disregard	1	2	0	3
Late Complaint Extensions	0	4	4	0
Media Inquiries and Interviews	1	37	37	1
Public Advisories	1	3	3	1
Best Practices	2	1	0	3
Interpretation Bulletins	2	0	1	1

Our Office strives to conclude files in as timely a manner as possible. Due to the complexity of some files and being a small staff, investigations can take several months to conclude. Below are average times in days it took us to complete various types files:

File Type:	Access Complaint	General Inquiry	Privacy Concern	Privacy Breach Notification	Comments on Proposed Legislation or Programs	Time Extension
Avg. # of Days	203	20	161	126	26	13

Informal Resolution Process

During our third year, we continued our efforts to resolve complaints by ensuring that those who requested information received all of the information they were entitled to receive. The public bodies have continued to work with our Office in an effort to resolve the complaints as they see it as an **effective method of resolving complaints**. The public bodies often thank us for our thoroughness and guidance, as they find our written comments helpful and to be a good resource to address similar issues in future access requests.

Individuals who have made access requests have also seen the **benefits of resolving**

complaints informally as they are either receiving additional information from the public bodies, or additional explanations as to why access to the requested information is refused. These individuals are nevertheless satisfied as they learn the reasons why access was refused.

In 2012-2013 alone, our **resolution of complaints continued with a high rate of success**; of the 27 complaint matters we have investigated only 4 have required formal recommendations to the public body.

Universities, municipalities and schools became subject to the *Act* on September 1, 2012, and

We received complaints involving all four provincial universities to disclose salaries and expenses of presidents and senior officials. This highlighted the public's interest in universities being open and transparent with this information.

our Office received the first access complaints with these **new public bodies** in the following months. Of six complaints with universities, four were informally resolved. We received ten complaints regarding municipalities, and worked closely with the municipalities to assist them in understanding and applying the rules of the legislation. Out of the ten, eight were informally resolved.

Proactive disclosure of information

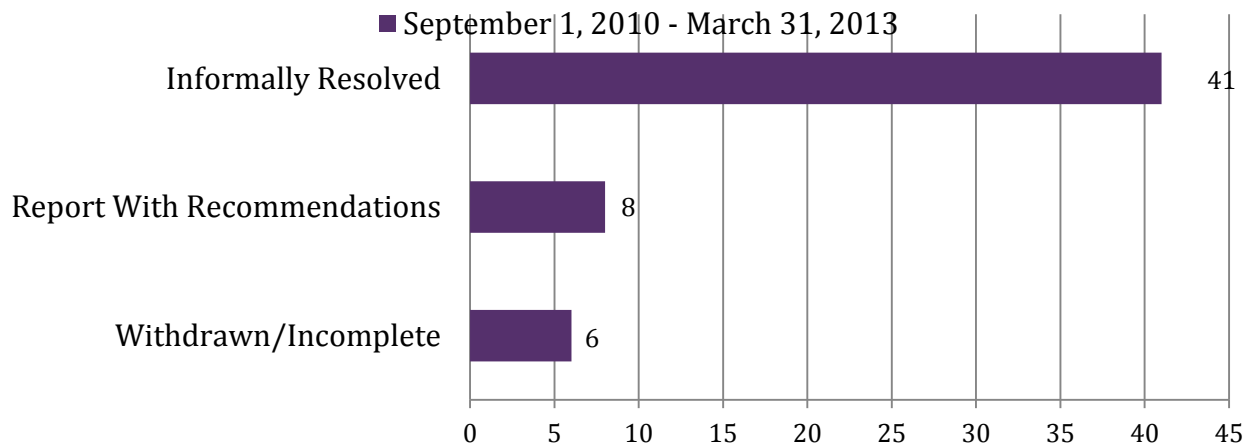
We encourage public bodies to consider **proactive disclosure** of certain information, such as annual reports, employees' and officials' salary ranges and expenses, public reports, etc.

More information being readily accessible to the public not only **increases transparency** but also may **reduce number of access requests submitted for processing**.

Two and a Half Years of Access Complaint Outcomes

Our Office concluded 55 access complaint investigations since the *Act* came into effect on September 1, 2010. Below is a breakdown of the outcomes of those complaints:

Access Complaints in the First 31 Months of the Office



- ❖ An access complaint that is **INFORMALLY RESOLVED** means that the public body has fully complied with the *Act*, and the applicant is either fully satisfied with the outcome or unsatisfied. If the Commissioner feels that a published report would provide education and guidance about the rules, then a **REPORT WITHOUT RECOMMENDATIONS** will be issued.
- ❖ A **REPORT WITH RECOMMENDATIONS** is issued when the public body has not fully complied with the *Act* and the Commissioner must formally recommend that the public body take action to meet its obligations under the *Act*.
- ❖ A **WITHDRAWN** complaint is when an applicant wishes not to go further with their complaint or pursue the matter, and an **INCOMPLETE** is when the applicant does not include all the necessary information in their complaint.

The Commissioner only issued 8 formal recommendations to public bodies, between September 1-2010 and March 31-2013 of which:
1 was **followed**
3 were **followed in part**
4 were not **followed**

Complex Investigations

The 2012-2013 fiscal years brought larger and more complex access complaints as those who request information are becoming more aware of their rights and more sophisticated in making requests. We investigated highly detailed and larger access complaints, with complicated nature of the information requested and exceptions to disclosure relied upon, not to mention the case of multiple complaints from a single applicant who submitted the same large requests to multiple public bodies.

Although the goal for these complex cases remained to informally resolve, these investigations required us to adjust our procedures in order to be more effective and timely as possible.

One case involved multiple complaints pertaining to the same requests made by one applicant to six separate public bodies. Before we could start our investigation, we had to determine whether we could accept the complaints as filed, given that they appeared to be filed outside of

Late Complaints – Commissioner’s discretion to accept late complaints or not

Someone not satisfied with a public body’s response to an access request can file a complaint with our Office and has 60 days from receiving the response to do so. While the Commissioner has discretion to accept late complaints, this is not done unless the applicant can make a case with exceptional circumstances for being late.

the time limits allotted by the *Act*, not to mention having to investigate the timeliness of various responses, and then analyse whether information was properly refused. We developed a test to make these determinations and found that the some were in fact timely due to the decisions reported by public bodies. Moreover, given that the access requests were large in scope and made to several entities, we first had to determine which public body had which records; this meant having a series of

meetings with each public body to assess how each had searched and located the relevant records, and then cross-referencing all the records in a master list to ensure that we were satisfied all records were identified and accounted for before we could even begin to investigate how access had been provided or refused in these cases. This case alone resulted in over a dozen separate rulings and decisions.

Issues Raised During Investigations

Draft documents – During our investigations, many public bodies were unsure of how to treat draft versions of official records, including letters, briefing notes, and reports. The *Act* does not automatically protect draft versions of records from disclosure, and these records must be considered on a case-by-case basis to determine whether access can be refused under the *Act*.

Briefing notes – Only the portions of Minister’s briefing notes that contain advice, opinions, recommendations or proposals for the Minister’s consideration can be protected under section 26 (“advice to a public body”) of the *Act*. Background and factual information are not protected.

Speaking notes – While speaking notes can often be withheld as advice to the Minister, it is important to verify whether they have been used by the Minister to speak publicly about an issue, in which case the information in the speaking notes would be publicly known and not need to be protected.

Consultants’ reports commissioned by government – Government sometimes engages external experts to conduct research and provide advice, feedback and recommended courses of action on complex matters. The resulting consultant reports should generally only be protected from disclosure where the report relates to an ongoing decision-making process.

Private business entities conducting business with government – When individuals or companies deal with public bodies in a business capacity, the information generated from these interactions is subject to possible disclosure under the *Act*. The *Act* recognizes that some information relating to private companies warrants protection from disclosure; however, some information about their dealings with the Province may be made available to the public. This encourages transparency and accountability in business dealings with the private sector by public bodies.

- **Information generally protected:** trade secrets, detailed business plans and financial statements, tender bid submissions and proposals, etc.
- **Information generally not protected:** nature and purpose of the contract, total value of the contract, contract terms and conditions, etc.

Public interest override/third party business information – In some cases, a public body must disclose private company business information when it is in the public interest to do so--

Public sector employee information/benefits – Public sector employees are paid from the public purse and, as a result, certain kinds of information about their employment and benefits may be made public to ensure accountability/transparency. Basic information such as job classification, salary range (but not exact salary), benefits, employment responsibilities and

travel expenses cannot be protected from disclosure under the Act. We have been encouraging public bodies to make this kind of information available to the public proactively where they are not already doing so.

Information to be published within 90 days – In certain cases, the *Act* allows a public body to refuse access to requested information where the public body has the intention of publishing that information within 90 days. This section is not meant to be used as grounds to delay access, but rather to give a public body the option of making the information available to everyone at a later date.

Meaning of “Act does not apply” – The *Act* applies to all records held by a public body except for certain kinds of records described in section 4 (such as court records, personal or constituency records of Ministers, Provincial Archive records, etc.). While some public bodies allowed us to review records that they believed fell within the scope of the exclusions found under section 4 so that we could determine whether access was properly refused, other public bodies challenged our jurisdiction to review records that they believed the *Act* did not apply to.

In our view, where a public body claims that a record is not subject to the *Act* under section 4, this is a decision that affects an applicant’s access rights and can be reviewed by our Office during a complaint investigation.

Duty to Assist and Meaningful Responses

The public bodies are becoming more aware of the importance of their **duty to assist applicants**, and overall most public bodies are fulfilling this requirement of the legislation. In that regard, we find that most public bodies are seeking clarification from applicants when needed and, as a result, they are conducting more proper and thorough searches for the records responsive to the requests.

“The head of a public body shall make every reasonable effort to assist an applicant, without delay, fully and in an open and accurate manner.”

- Section 9 of the Act

During our work with local public bodies, such as municipalities, we have noted that the duty to assist seems to come naturally to them as they work more closely with members of the public, especially in smaller communities.

Time extension applications

Of the 10 time extension applications we received from public bodies this year, most were based either on the large volume of records involved or additional time need to notify and receive representations from third parties or consult with another public body before making a decision about access.

When public bodies cannot fully respond to a request by the deadline imposed by the Act, they can **extend the deadline** for responding by up to 30 days under certain circumstances, and must notify the applicant of this extension. By doing so, public bodies are making sure that applicants are aware of the extended timeframe, as well as when they can expect a response. If a public body believes it will require more than an additional 30 days to respond, it may apply to the Commissioner for a further extension of time.

With a view to provide timely access to the applicant, however, public bodies can also provide partial responses where possible. We encourage this practice, as it ensures that access is not delayed for information that can be released ahead of the extended deadline.

In keeping with the duty to respond to requests in an open and accurate manner, we encourage public bodies to provide lists of records responsive to the request in order to make responses more meaningful. The more

explanation provided to an applicant as to why access to the information is being refused, the greater the likelihood that the applicant will understand the refusal, making the applicant less likely to file a complaint.

Records Management

Public bodies must have a comprehensive records management system in place and take steps to ensure that their decisions are properly documented for the official record.

Whereas a public body does not document its decisions or keep copies of its records, it not only raises questions about accountability but also makes important information unavailable to the public.

Privacy Breach Notifications

Public bodies may choose to notify our Office of privacy breaches, which occur when a public body discovers that personal information has been stolen, lost, improperly disposed of or disclosed to or accessed by an unauthorized person. This notification allows us to assist them in **containing the breach and implementing corrective measures** to prevent future breaches.

Privacy breach notifications are not mandatory under the *Right to Information and Protection of Privacy Act*, but many public bodies opt to notify our Office when a breach occurs to benefit from our guidance. Although it is not subject to legislation or to the Commissioner's oversight, we were also notified by Elections New Brunswick of two privacy breaches so that the Commissioner could **independently investigate and provide assistance** and guidance.

In total, our Office was notified of nine privacy breaches under the *Right to Information and Protection of Privacy Act* between April 1st, 2012 and March 31st, 2013.

- There was one **Misdirected Communication, Unauthorized Disclosure, Same Name Mix-Up, Stolen Equipment, and Snooping** breach, each, this past year.
- There were two **Abandoned or Lost Records** breaches and two **Additional Individual's Information Given** breaches this past year.

While most privacy breaches occur due to human error, they can also happen as a result of stolen equipment, or staff snooping in records containing personal information.

Privacy Concerns

When individuals contact us stating that they believe a privacy breach has taken place within a public body, or that its policy or practice may be in contravention of the legislation, we raise their concern with the public body in question and review its practices regarding the handling of personal information.

Where necessary, we remind public bodies of their duty to only collect, use, disclose or access the minimum amount of personal information necessary to complete their work, and to get consent from the individual whenever possible. We also recommend corrective measures to prevent future breaches from taking place.

Between April 1, 2012 and March 31, 2013, our Office concluded 15 privacy concern files under the *Right to Information and Protection of Privacy Act*.

Many concerns raised with our Office involve the question of how much personal information individuals are required to provide in order to participate in government programs. Another common issue is the question of when an individual's consent is required for personal information to be shared.

- Seven of these privacy concerns were **unfounded**,
- Four of the privacy concerns were **withdrawn or abandoned**,
- Three of the privacy concerns had to do with **unauthorized disclosure**, and
- One of the privacy concerns had to do with **unauthorized collection**.

Types of Privacy Concern Outcomes

Three of those concerns were the results of **unauthorized disclosure**, such as when a public body mistakenly believes it has authority to share personal information with another organization.

One privacy concern resulted from a public body's **unauthorized collection** of personal information. In this case, the public body was collecting more personal information than was necessary to carry out the purpose for which it was collected.

Seven of the privacy concerns concluded by our Office were deemed to be **unfounded** following our investigation; that is, the handling of personal information that had concerned the individual was found to have been permitted under the *Act*.

Four of the privacy concerns were **withdrawn or abandoned** by the individual. Privacy concerns are most often withdrawn because individuals do not want their names shared with the public body in connection with the privacy concern; however, our Office is unable to investigate without sharing their names as the public body would not be able to identify the incident in question.

In some cases, an unfounded privacy concern still leads to identifying practices that, though permitted by legislation, can be modified to better protect the privacy of New Brunswickers.

For example, other provincial laws require Service New Brunswick to make mortgage information publicly available, but concerns raised by members of the public have prompted Service New Brunswick to work with our Office to amend how much personal information is published while still providing adequate disclosure of property interests.

Personal Health Information Privacy and Access Act

The *Personal Health Information Privacy and Access Act* sets out rules for custodians, such as doctors, nurses, hospitals, dentists, physiotherapists, nursing homes, and other health care providers, for the handling and protection of personal health information, including providing access to one's own **personal health information**.

The Commissioner's mandate under the *Act* includes many different areas of responsibility and although many are similar to those under the *Right to Information and Protection of Privacy Act*, the focus here remains on ensuring that custodians keep health care information of patients and clients confidential at all times, thereby protecting privacy and maintaining a high level of public trust that is essential for a well-functioning health care system.

Breakdown of files handled under the Act in 2012-2013

We opened **154 new files** under the *Personal Health Information Privacy and Access Act* between April 1-2012 and March 31-2013 while continuing our work under this statute.

	Files carried over from previous year	Files opened 2012-2013	Files Closed 2012-2013	Files remaining open at year end
Access Complaints	4	4	4	4
General Inquiries	11	72	56	27
Privacy Complaints	6	24	13	17
Privacy Breach Notifications	18	50	15	53
Comments on Proposed Legislation or Program	0	1	1	0
Media Inquiries and Interviews	1	1	2	0
Best Practices	3	2	0	5

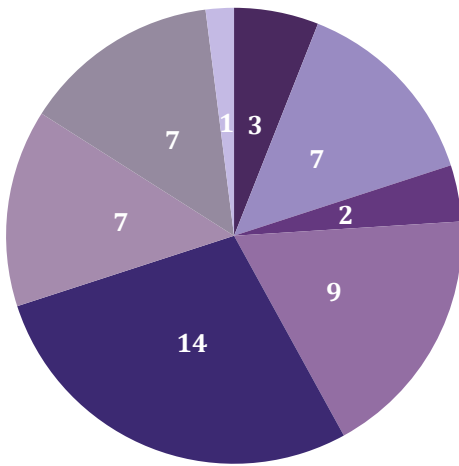
The following table shows the average length of time taken to conclude these types of files:

Type of File	Access Complaints	General Inquiries	Privacy Complaints	Privacy Breach Notifications	Comments on Proposed Legislation or Program
Avg # days	146	29	181	243	7

Privacy Breach Notifications

The *Personal Health Information Privacy and Access Act* requires custodians to notify **both the Commissioner and those affected** whenever personal health information is lost, stolen, or disposed of, or disclosed or accessed in a manner contrary to the Act. Our Office was notified of **50 privacy breaches** of various descriptions during that fiscal period. On the following page we illustrate and explain the differences between the types of breaches and how often we have come across them in the past year.

Types of Breach Notifications



- Unauthorized Disclosure
- Misdirected Communication
- Same Name Mix-up
- Additional Individual's Information
- Abandoned or Lost Records or Information Left in Equipment
- Gossip
- Snooping
- Records Damaged by Flooding

Unauthorized Disclosure: when personal health information was disclosed to someone who was not permitted to see it.

Misdirected Communication and same name mix-up: cases where personal health information was sent to the wrong individual.

Breaches of **Additional Individual's Information** occur when another person's information was accidentally included along with information intended for another.

Abandoned or Lost Records or Information Left in Equipment: incidents occur when custodians cannot locate personal health information that should be in their custody, or when records are discarded inappropriately/ improperly stored or destroyed, leaving them at risk of further disclosure.

Gossip: health care providers or their staff discuss patient/client information for a purpose other than the provision of health care.

Snooping: accessing a patient or client health care file outside of the performance of one's work duties.

Records Damaged by Flooding was a privacy breach incident that took place when a hospital flooded and paper records, not previously saved electronically, were damaged.

Privacy Complaints

The *Personal Health Information Privacy and Access Act* gives individuals the **right to file a privacy complaint** with our Office if they believe that a custodian has collected, used or disclosed their personal health information in an improper manner, or where the individual believes the custodian failed to implement appropriate safeguards to protect his or her personal health information. Some of the privacy complaints we received resulted from being notified by the custodian who was responsible for the privacy breach, and in most cases, we had already been notified of the incident by the custodian.

When a privacy complaint is filed, we notify the custodian of the details of the complaint and continue our investigation with the custodian. If we did not have prior knowledge of the incident, we contact the custodian without delay and begin our investigation. Our role is to require the custodian to conduct its own internal investigation and provide us with those results, after which we independently verify what happened. We also look into the custodian's privacy practices and conclude with findings as to whether a breach took place, with **corrective measures to prevent future incidents**. We often recommend that the custodian remind staff of the importance of keeping patient/client information safe, secure and confidential at all times, with a view to only use the information when they are authorized to do so in their work.

In cases where multiple complaints have resulted from a single privacy breach notification that affects a large number of individuals, our practice is to publish the **Report of the Commissioner's Findings with recommendations** (translated and loaded on our website) with a view to inform everyone affected and the public at large; more importantly, serving as notice that such actions will be investigated, uncovered, and not tolerated in the future.

Whenever recommendations are made, the custodian is given a timeline to implement them and then to advise our Office when that has taken place. It is important to note that we do not fully conclude the privacy complaint files until the custodian **confirms that all recommendations have been followed**.

In the 2012-2013 fiscal period, we received **24 privacy complaints** from various individuals under the *Personal Health Information Privacy and Access Act*, of which 12 were for snooping into health care records, 4 resulting from unauthorized disclosure, 4 cases where there was not the requisite consent to handle the information, and the remaining 4 had no merit.

Types of Privacy Complaints

The **snooping** complaints are usually derived from individuals who were victim of a custodian or staff member having accessed their medical record without prior knowledge or consent. We consider these cases to be the most serious of privacy breaches, in that, if true, it revealed an intention to breach the privacy of that individual, a serious matter indeed. Also serious are those cases where the custodian handled the individual's health care information without consent or believing it was allowed to rely on implied consent, thereby leading to a **privacy complaint** of gossiping or unauthorized use or disclosure. These privacy complaints investigations require us to carefully examine the facts surrounding how consent was first obtained in order to assess whether the consent was still valid when the individual's information was used or shared.

Despite the nature of any of the privacy complaints cases we receive, we examine each one with the same degree of attention, to obtain the correct facts and satisfy ourselves as well as those who complained whether the incident was the result of an unintentional error due to lack of controls that will not be repeated, or worse, was the result of an intentional disregard for the privacy of the individual, resulting in recommendations with more serious implications.

Snooping cases

The number of complaints we receive regarding snooping in health care records do not accurately reflect the number of individual who were actually affected by such events. According to the notification we received of the number of people affected in snooping cases involving multiple records, approximately 5% of those affected will take action and file a formal complaint with our Office. As a result, while we received 13 formal complaints regarding unauthorized access to health care records, those complaints were only a small measure of the actual numbers of those affected, which we included in our broader investigation of snooping into hundreds of health care records. In one case alone, about 150 individuals were notified that their medical record had been improperly accessed and only nine of them filed complaints with us. Notwithstanding the number of formal complaints, our work encompassed the entire incident, and we looked into each event of unauthorized access. Our findings were shared with those who formally complained, but also with those who did not by making our findings public.

General Inquiries

We continue to receive a significant number of general inquiries under both statutes. General inquiries **range from simpler questions**, such as how to make access requests, how to file complaints, how to access one's medical records, and who is subject to the statutes, **to more specific and complex questions of interpretation** of various rules under this legislation.

As we noted a greater awareness on the part of the public regarding procedures as to how to go about obtaining information from various public bodies, we received fewer inquiries on that score; furthermore, by having posted many helpful questions and answers, forms and processes on our website, a lot of those inquiries were addressed.

The more **complex inquiries** came from both members of the public and those subject to the legislation, as well as law firms, and private groups about interpretations of various provisions: whether consent is required to collect, use or disclose an individual's information in certain circumstances; what are the privacy implications for electronic storage of sensitive records; whether video surveillance is permissible in certain locations, including in work settings or specialty centres; when it is proper to disclose personal information to law enforcement, and so on. While we endeavoured to answer most general inquiries quickly, the more complex inquiries required significant time and effort on our part as we **thoroughly researched the question before providing the correct answer**.

Below are some of the topics we were asked to look into and the answers we provided.

Social Media and Privacy

Social media, such as Twitter and Facebook, is widely used by members of the public and is also used by many organizations subject to access and privacy legislation as an important tool for reaching the general public. Information can be shared with a large group of people and social media guarantees that this can be done instantly. While social media is convenient, those using it must **remain mindful of its potential implications for protection of privacy**.

If a person's information is **collected, used or disclosed in an unauthorized manner** through social media by an individual or organization that is subject to the statute, it is considered a breach of privacy, and the Commissioner can investigate the matter as she would any other privacy breach.

Organizations using social media must therefore **ensure the protection of sensitive information** in the same manner as they would outside of those parameters.



This is done by:

- Having privacy procedures that clearly outline appropriate use of personal information on social media,
- Training staff on those procedures to clarify responsibilities at the outset, and,
- Having employees sign an oath of confidentiality.

Deceased Individuals' Information

We have received multiple inquiries about **whether access may be granted to a deceased individual's personal information or personal health information**. There are different standards for the protection of personal information under the *Right to Information and Protection of Privacy Act* and for the protection of personal health information under the *Personal Health Information Privacy and Access Act*.

The *Right to Information and Protection of Privacy Act* deems that the disclosure of personal information about a person who has been deceased for more than 20 years is not an unreasonable invasion of that person's privacy. Before that time, however, the deceased person's personal information must remain protected and can only be shared in very limited situations.

On the other hand, the *Personal Health Information Privacy and Access Act* does not apply to records that were created more than 100 years ago, or to an individual's personal health information after 50 years have passed since that person's death. Despite that rule, there is a **limited right of access** to a deceased person's personal health information before 50 years have passed since his or her death. The personal representative of the deceased may request access to the deceased's personal health information if it is needed to carry out the administration of the estate.

In other cases, a custodian who has a deceased's personal health information in its records may share some information on the following basis:

- To **identify the deceased**,
- To **inform someone, if appropriate**, that the individual is deceased or of the circumstances of the death,
- To the deceased's personal representative but only in connection with a task that is required for the **administration of the deceased's estate**,
- To a spouse, common-law partner, sibling or descendant of the deceased **if needed to make decisions about his or her own health care or the health care of his or her child**,

- If the disclosure is **necessary to provide health care** to a spouse, common-law partner, sibling or descendant, or
- For **research purposes**.

Consent and Privacy

We also encountered many questions surrounding consent and privacy, and we observed that both of these concepts were **widely used, but not always fully understood**.

Privacy is based on the notion that personal **information belongs to the individual** and not to those who maintain it. In that regard, public bodies and custodians must respect individuals' ownership of their personal information and their **right to know and understand why and how it will be collected, used and disclosed**.

In the foreground from which privacy is respected originates consent of the individual that must be obtained before collecting, using or disclosing personal information wherever possible. We often pointed out that in order **to provide consent**, an individual must first *understand*:

- **why** his or her personal health information must be collected (for what purpose);
- **what will be done** with the information once it has been collected;
- **whether the information will be shared with others** in order to accomplish the purpose, and if so:
 - **with whom, for what purpose, when and what information will be shared**.

Consent Forms

When a public body or custodian uses a complicated consent form, our experience has shown that individuals do not always understand what they are consenting to. We therefore worked with public bodies and custodians to ensure that they are not always reliant on overly complex forms, and encouraged them to have discussions with individuals so that they would be better informed and better suited to provide consent, especially when having to provide consent in writing.

WHO COMPRISED THE TEAM FROM APRIL 2012 TO MARCH 2013?

During that time, the Office of the Access to Information and Privacy Commissioner continued to benefit from the valued work of a team of dedicated individuals:

Legal Counsel and Investigators

Kara Patterson
Chantal Gionet (from June 2012)
Anik Cormier (from February 2013)

Intake Officer

Norah Kennedy

Portfolio Officer

Ben McNamara

Researcher

Céline Bastien (from May to October 2012)

Administrative Assistant

Lucrece Nussbaum

FINANCIAL INFORMATION - *fiscal year ending March 31, 2013*

Employee Salary & Benefits	\$	442,768.00
Office Rent, Travel & Other Services	\$	122,734.00
Materials & Supplies	\$	4,335.00
Furniture & Equipment	\$	16,113.00
TOTAL EXPENDITURES:	\$	585,950.00

Have Questions or Concerns? *Please Contact Us:*

Office of the Access
to Information and
Privacy Commissioner

New Brunswick




Commissariat à l'accès
à l'information et à la
protection de la vie privée

Nouveau-Brunswick

65 Regent St. Suite/bureau 230
Fredericton, NB E3B 7H8

 506-453-5965 | Toll-free/Sans-frais: 1-888-755-2811

 506-453-5963

 www.inf-priv-nb-ca

Access.info.privacy@gnb.ca | accès.info.vieprivée@gnb.ca