

NOTE TO COMMISSIONER

From Valerie Lawton c.c. Anne-Marie Hayden, Daphne Guerrero
Date November 4, 2016
Subject Plan for the creation and management of an OPC Facebook Page

Commissioner,

Following your agreement on the recommendation to create a Facebook Page to further our public outreach efforts, we have updated the strategy outlining how the OPC would use Facebook. You will recall that you had reviewed and approved an earlier version of this strategy in August, which had been reviewed by both the Office's CPO and discussed with the Privacy Accountability Working Group (PAWG).

The updated strategy now includes a section outlining the OPC's overall approach to developing and managing the OPC's Facebook Pages. This new section contains:

- A proposed approach to sharing and engaging
- Foundational elements to launch the page (OPC Facebook Comment Policy, OPC Facebook Privacy Notice, Posting guidelines / Service standards)
- Compliance with Government of Canada policies and guidelines (Identity, Official Languages, Accessibility, Publishing, Account configuration and compliance)
- Development of the Facebook Page (Development and branding, Account Verification)
- Ongoing management (Posting, Approval process, Daily management of Facebook page)
- Evaluation

We are seeking your approval for the overall approach and the following documents included in the strategy: OPC Facebook Comment Policy and OPC Facebook Privacy Notice.

Also attached for your approval is a proposed launch strategy for the Facebook Pages. We are targeting a launch on December 5.

We would propose to conduct a demonstration of the Page for you at an upcoming bilat.

Revisions and/or approval

- I approve this strategy and launch plan.
- I have revisions and wish to see a new version of the strategy and launch plan.
- I have questions/concerns regarding this file and wish to discuss.

Comments :

Signature :

NOTE TO COMMISSIONER

cc: Anne-Marie Hayden

From Valerie Lawton

Date Oct. 31, 2016

Subject Media lines – FTC Ashley Madison

Please find attached draft lines related to the FTC's upcoming launch of its work on the Ashley Madison matter.

We've consulted with PIPEDA, Policy and Legal to develop the lines.

Brent has proposed that, once you approve, we should run the lines by the FTC before sharing publicly.

—

Approval and comments

- I have approved the lines
- I have made changes and wish to see a new version
- I wish to discuss

Comments:

Signature:



1/11

7777 - 6 - 170865

Key Messages

We were pleased to have been able to cooperate with the FTC on this matter. The ability to coordinate, share information and discuss analyses, was helpful during our investigations.

The FTC conducted its own investigation, based on the consumer protection legislation that it enforces, and came to an agreement in principle with the company to reimburse certain fees paid by customers on the site.

In the joint Canada-Australia investigation, which examined the company's compliance with privacy laws, we too were able to achieve an outcome that will lead to improved privacy and security practices at the company.

As you may know, our office has also highlighted the broadly applicable "lessons learned" from that investigation to help *all* companies operating online ensure they meet their privacy obligations.

Qs and As

Is it odd/problematic/etc that the U.S. will collect heavy fines and the OPC won't even though this is a Canadian company?

The FTC conducted its own investigation, based on its consumer protection legislation, and came to an agreement in principle with the company to provide restitution for-certain fees paid by customers on the site.

In the joint Canada-Australia investigation, we were able to achieve an outcome that will lead to improved privacy and security practices at the company – to the benefit of Canadians and other users.

You're correct that our Office does not currently have order-making powers or the ability to impose fines or penalties.

Many of our domestic and international partners currently do have such powers, as do regulators in the realm of consumer protection. It does raise questions with respect to PIPEDA enforcement powers, and this issue is one that could be examined in future discussions on potential PIPEDA reforms.

It is also worth noting that the current enforcement model and powers under PIPEDA is something we are asking for feedback on in the context of our public consultations on the consent model.

If pressed on fines/enforcement powers ...

We're consulting on this issue so it would be premature to offer a view on the issue at this point.

If the OPC had the authority to impose fines and other countries did as well, is there a risk of piling on?

We see an increasing number of privacy issues affecting individuals in multiple jurisdictions. Therefore, it's increasingly important that there be awareness, collaboration and communication between international partners when an issue is being investigated by multiple bodies.

Such collaboration took place in the Ashley Madison matter between our Office, our Australian counterpart and the US FTC.

Where several regulators have the power to impose fines, we believe it would be appropriate for data protection authorities to exercise their powers in the context of their own legislation, but taking into account the more global impact as much as possible.

Collaboration and communication among enforcement bodies – when confidentiality rules allow – can help ensure an appropriate, balanced outcome that achieves compliance and ensures individuals' privacy rights are protected.

What could we say about the complementarity of remedies under the current law? Other than fines, how is the U.S. order similar and/or different from ours or the Australians'?

Given that the three offices collaborated on this matter, it is not surprising that many of the findings are consistent.

Our three offices had key common interests in this matter, in particular the need for adequate security safeguards.

To this end, we are confident that our remedies for addressing ALM's safeguard failings also served to address many of the concerns of the FTC.

The FTC is a consumer protection agency and it therefore approaches issues from a consumer protection perspective. As a consequence, much of the FTC focus in this case was on misrepresentations; unfair security practices; and consumer injury.

That being said, there is overlap in the area of privacy and consumer protection – for example, we all took issue with the phony security trustmark.

Given that the FTC examined issues from a consumer protection perspective, the FTC Order does also include elements not covered in our compliance agreement – most notably, the prohibition against misrepresentation relating to “engager profiles” and the monetary judgement comprising both “equitable monetary relief” and restitution.

Similarly, OPC's joint investigation with OAIC addressed complimentary issues not covered by FTC's investigation, specifically, relating to accuracy (with respect to non-user information) and over-retention of inactive and deactivated accounts. (Australian and Canadian privacy laws both have specific requirements relating to these issues.)

At the end of the day, our combined remedies have achieved a comprehensive outcome – we have not only dealt with structural privacy safeguard failings, but also issues touching on retention, accuracy and misleading advertising.

Specifics:

- The FTC came to an agreement in principle with the company to provide restitution for certain fees paid by customers on the site.
- In the joint Canada-Australia investigation, we examined the company's compliance with privacy laws and we were able to achieve an outcome that will lead to improved privacy and security practices at the company.
- As you may know, our office has also highlighted the broad "lessons learned" from that investigation to help *all* companies operating online ensure they meet their privacy obligations.

BACKGROUND FOR YOUR INFORMATION:

Monetary implications of FTC order

The monetary implications of the FTC's settlement with Ruby can be lumped into one of two categories, neither of which are characterized as "fines" by the FTC:

- i) **Restitution:** These are fees to be paid by the company to the FTC to reimburse customers.
 - a. Ruby has agreed to pay the FTC and States that have collaborated on the investigation a sum of \$1.6M USD. The figure represents both money consumers spent on purchasing the \$19 "Full Delete" feature as well as money consumers spent to purchase credits to communicate with the engager profiles. The sum represents the maximum amount of money the FTC's economist determined the company had the ability to pay without going bankrupt.
- ii) **Equitable monetary relief:** These are fees to be paid by the company The FTC for use for restitution, for providing to the U.S. Treasury (in the event that the sum is too small to be used for restitution), or to be used for consumer education.
 - a. The FTC order mandates that Ruby pay \$17.5M USD in equitable monetary relief (though the collaborating States with whom the FTC is collaborating are likely to refer to this as a civil penalty, which is more akin to a fine). As Ruby has demonstrated an inability to pay this amount, this will be characterized as a "suspended judgement" in the FTC's order - Ruby will only have to pay this amount (minus the \$1.6M USD in restitution) if it is later uncovered that the company was not truthful in the financial statements it gave the FTC.
 - b. The FTC order further states that Ruby must pay the FTC an amount of \$7.5M CAD currently residing in a trust fund only if Ruby comes into possession of the funds. This is also characterized as equitable monetary relief.

If Ruby violates the terms of the order in general, then the FTC would be in a position to bring a separate enforcement action.

Broad themes of FTC order

- I. Prohibition against misrepresentations (overlap with our recommendations on transparency with the exception of the "engager profile" issue, which is unique to the FTC and is covered under "user profiles" below)
 - o Network security
 - o User profiles
 - o Terms and conditions for deleting profiles
 - o Data security seal
- II. Mandated security program (broad overlap with our information security recommendations)
 - o Designation of individual responsible for the program
 - o Risk assessments
 - o Reasonable safeguards
 - o Reasonable steps to select service providers
 - o Evaluation and adjustment of program in light of testing and monitoring
- III. Data security assessments by third party (overlap with our information security recommendations)

- IV. Monetary judgement – described above
- V. Customer information - Ruby can't use customer info obtained prior to the Order, except if terms I-III above are respected
- VI. Compliance reporting – Initial compliance report followed by twenty years of compliance notices for any changes to organization
- VII. Recordkeeping – Twenty years of recordkeeping
- VIII. Compliance monitoring – Ruby must, at FTC's written request at any time, submit additional compliance reports or other requested information

7777-0-174219

Commissariat
à la protection de
la vie privée du Canada



Office of the
Privacy Commissioner
of Canada

NOTE TO COMMISSIONER

From: Steven Morgan

Date: December 9, 2016

Subject: Letter of advice-Privy Council Office

Please review letter of advice to PCO regarding the
mydemocracy.ca survey.

Approval and comments

I have approved *late Dec 9 draft attached*

I have approved and provided revisions to the letter of advice

I would like to discuss.

Comments :

Signature :

**Pages 10 to / à 13
are withheld pursuant to sections
sont retenues en vertu des articles**

16.1(1)(d), 21(1)(b)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

s.20(1)(b)

s.20(1)(c)



Office of the
Privacy
Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Security Classification/ Désignation Classification/désignation sécuritaire	Total Pages Pages totales
Protected B	5

BRIEFING NOTE

NOTE D'INFORMATION

PURPOSE / OBJET:

During a discussion with the PIPEDA Branch regarding the [redacted] lawful access matter, you requested further information on the approach taken by 'U.S. tech giants' and the existence of jurisprudence. This memo sets out the approach taken by large U.S. based technology companies in responding to information requests from authorities outside of the U.S. and also summarizes the decision of the U.S. Court of Appeals in a case involving user data stored by Microsoft on a server in Ireland. Finally, attached for your consideration and approval is the proposed letter to [redacted] closing the file.

OVERVIEW / APERCU:

We conducted a review of transparency reports and other publicly available information from select technology companies in order to consider how requests for information from foreign authorities may be treated. From the information available, Facebook appears to take a similar approach to [redacted] by considering the laws of the requesting state. Below are excerpts from each company's policies for your information. It is worth noting that owing to the global reach of the companies considered, it is unclear from the information available to us whether requests are received by the local subsidiaries or headquarters (or both) and what impact that has on the company's requirements for requestors (e.g. MLAT, or applicable local laws).

Facebook

We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.¹

International Legal Process Requirements: We disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.²

¹ *How do we respond to legal requests or prevent harm* Facebook Data Policy, available online at <https://www.facebook.com/policy.php>

² *Information for Law Enforcement Authorities* Facebook, available online at <https://www.facebook.com/safety/groups/law/guidelines>

Twitter

Requests for Twitter Account Information - Requests for user account information from law enforcement should be directed to Twitter, Inc. in San Francisco, California or Twitter International Company in Dublin, Ireland. Twitter responds to valid legal process issued in compliance with applicable law.

Private Information Requires a Subpoena or Court Order - Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process – or in response to a valid emergency request, as described below.

Contents of Communications Requires a Search Warrant - Requests for the contents of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter.³

Google

What does Google do when it receives a legal request for user data? Respect for the privacy and security of data you store with Google underpins our approach to producing data in response to legal requests. When we receive such a request, our team reviews the request to make sure that it satisfies legal requirements and Google's policies. Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorised official of the requesting agency and issued under an appropriate law.

[...]

Using Mutual Legal Assistance Treaties (MLATs) and other diplomatic and cooperative arrangements, non-U.S. agencies can work through the U.S. Department of Justice to gather evidence for legitimate investigations.

[...]

On a voluntary basis, we may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country.

[...]

Is the MLAT the only way for governments outside the U.S. to get information from U.S. companies?

No. There are many ways that other countries can obtain information from companies like Google outside of the MLAT process, including joint investigations between U.S. and local law enforcement, emergency disclosure requests and others.⁴

Apple

When we receive information requests, we require that it be accompanied by the appropriate legal documents such as a subpoena or search warrant. We believe in being as transparent as the law allows about what information is requested from us. We carefully review any request to ensure that there's a valid legal basis for it.⁵

For government information requests, we comply with the laws pertaining to global entities that control our data and we provide details as legally required. For content requests from law

³ *Guidelines for Law Enforcement Twitter*, available online at <https://support.twitter.com/articles/41949#8>

⁴ *Legal Process Google Transparency Report*, available online at https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

⁵ *Apple's commitment to your privacy Apple*, available online at <http://www.apple.com/ca/privacy/>

enforcement agencies outside the U.S., with the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), Apple will only provide content in response to a search warrant issued pursuant to the Mutual Legal Assistance Treaty process or through other cooperative efforts with the United States Department of Justice.⁶

Amazon

Non-U.S. requests. Non-U.S. requests include legal demands from non-U.S. governments, including legal orders issued pursuant to the Mutual Legal Assistance Treaty process or the letters rogatory process. Our responses to these requests depend on the nature of the request. Amazon objects to overbroad or otherwise inappropriate non-U.S. requests as a matter of course.

Amazon Law Enforcement Guidelines: Requests from Non-U.S. Law Enforcement - A non-U.S. law-enforcement agency seeking to obtain data from Amazon must work through the available legal and diplomatic channels in its jurisdiction, including through bi-lateral or multi-lateral legal assistance treaties ("MLATs") or letters rogatory processes. Such international requests may be made to the U.S. Department of Justice Office of International Affairs.⁷

Case law

Below is a summary of the Microsoft decision⁸ received from Sidley Austin, an American firm which provides us with an annual update on US privacy law.

Second Circuit Declines to Extend Warrant Provision of SCA to Data Stored on Foreign Servers. On July 14, 2016, the U.S. Court of Appeals for the Second Circuit issued a long-awaited decision that—to the surprise of many observers—rejected the government’s construction of the Stored Communications Act (SCA) and instead embraced a more restrictive view that Microsoft had advanced, backed by much of the tech industry and many privacy groups. *Microsoft Corp. v USA, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* (2d Cir. July 14, 2016)(Docket No. 14-2985). (Sidley Austin LLP represented a number of *amici* in support of Microsoft before the Court of Appeals and District Court.) The decision holds that electronic communications that are stored exclusively on foreign servers cannot be reached by U.S. prosecutors under the SCA’s warrant provisions—not even where the warrant is served on a U.S. provider that can access the foreign-stored information and deliver it to U.S. officials, by using computers and personnel based here in the United States.

The case involved a warrant requiring Microsoft to produce the communications of one of its web-based email customers. Microsoft disclosed all relevant U.S.-stored information, but objected that all of the e-mail content information was stored on a server in Ireland. In Microsoft’s view, that foreign storage placed the information beyond the proper reach of

⁶ *Legal Process Guidelines*, Apple, available online at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>

⁷ *Amazon Law Enforcement Guidelines*, Amazon, available online at https://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

⁸ *Microsoft v United States of America*, [2016] Case 14-2985, available online at <https://www.documentcloud.org/documents/2993634-Microsoft-ca2-20160714.html>

s.20(1)(b)

s.20(1)(c)

the U.S. warrant, and required U.S. prosecutors to work with Irish authorities to secure the information in a manner consistent with Irish laws. This issue was central because of a U.S. legal principle called the presumption against extraterritoriality. Reasoning that “the relevant provisions of the SCA focus on protecting the privacy of the content of a user’s stored electronic communications,” [Op. 33]. The court sided with Microsoft and held the warrant could not be used to compel disclosure of information stored in Ireland.

Key factors in the Court’s decision were the language used in the *Stored Communications Act* (specifically the meaning of the term “warrant”) and the strong presumption against extraterritorial effect in American law. The case does not stand for the general proposition that an American court could never issue a judicial authorization with extraterritorial effect, and leaves open the possibility that a differently drafted statute might permit such authorization.

The U.S. Justice Department filed an appeal with the U.S. Supreme Court on October 13, 2016.

RECOMMENDATION:

I recommend that you approve the attached letter to [REDACTED] closing this matter.

CONSULTATIONS: Michael Sims

DISTRIBUTION:

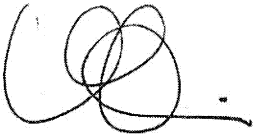
Rédigé par / Prepared by	Date	Revisions
Jennifer Rees-Jones	October 26, 2016	
Approved by – Approuvé par		Date
Brent Homan <i>Director General – PIPEDA Investigations</i>		

Approuvé par / Approved by

Date

Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s).

Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s):
Commentaires ou des instructions supplémentaires / Additional Comments or Instructions:



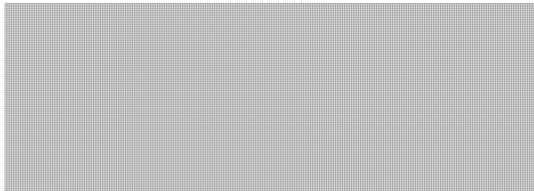
1/11/16

Daniel Therrien

Le commissaire à la protection de la vie privée / Privacy Commissioner

s.20(1)(b)

s.20(1)(c)



NOV 10 2016

Dear [REDACTED]

This is further to our letter sent June 30, 2016, and subsequent meeting with [REDACTED] on August 30, 2016, regarding [REDACTED] lawful access team.

We are writing to inform you that our Office has decided not to pursue the matter further at this time. Our decision was formed on the basis of explanations and assurances you provided regarding [REDACTED] approach to responding to requests from law enforcement. Specifically, our Office is given to understand and will rely on:

- [REDACTED] assurance that it does not disclose the personal information of its customers without lawful authority. Specifically, [REDACTED] relies on: (i) informed consent (as set out in terms of service and end user agreements); and (ii) the exemptions to consent set out in paragraphs 7(3)(c) and 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*.
- [REDACTED] assurance that the mutual legal assistance treaty (MLAT) regime is not being bypassed. [REDACTED]
- [REDACTED] assurance that the law of the requesting jurisdiction is followed. To safeguard this commitment, it engages local lawyers to provide legal advice on what the law of that jurisdiction requires, and consults with the International Assistance Group at the Department of Justice and the province, and the local Royal Canadian Mounted Police Liaison Officer posted to the local embassy, to ensure that the requesting organization is the appropriate agency within that country to make such a request.

s.20(1)(b)

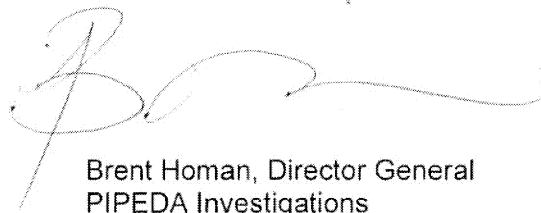
s.20(1)(c)

Notwithstanding our decision to close this matter, we are taking this opportunity to strongly urge [REDACTED]

The Office of the Privacy Commissioner of Canada has been calling for greater transparency in the context of surveillance and intelligence-gathering for many years. Transparency reports from private sector organizations can provide Canadians with timely, complete and accurate statistical information about how often and in what circumstances businesses provide customer information to law enforcement and security agencies. Such reports allow consumers to make informed choices and help support public discussion about privacy issues. While we appreciate the challenges you raised (namely, [REDACTED] given the potential value to Canadians, we are confident that you can find ways to achieve the objective of transparency reporting with reasonable economy.

As we mentioned during the meeting, there are resources available to assist in the transparency reporting process. Specifically, Innovation, Science and Economic Development Canada has developed Transparency Reporting Guidelines¹ for businesses to report on the number and types of requests they receive from government agencies to access customer information. Also, our Office has developed a comparative analysis² of transparency reports voluntarily published by some private sector companies over the last two years. We hope you will utilize these resources.

Sincerely,



Brent Homan, Director General
PIPEDA Investigations

¹ *Transparency Reporting Guidelines*, Innovation, Science and Economic Development Canada, available online at <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html>.

² *Transparency Reporting by Private Sector Companies*, Office of the Privacy Commissioner of Canada, available online at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2015/transp_201506/.

OPC Facebook Page Strategy

Table of Contents

Background	1
Objectives.....	2
Additionally:	2
Consultations	2
Considerations	2
Overall approach.....	5
Communicating and Engaging	6
Foundational elements	6
Compliance with Government of Canada policies and guidelines	9
Development of the Facebook Page.....	10
Launch	11
Ongoing management	11
Evaluation	12
Critical path.....	14
Annex A – Examples of posts	15

Background

The OPC will be establishing a Page on Facebook for the purposes of communicating with Canadians as part of the Office's outreach efforts. In particular, the page will focus on communicating with parents of children and young people, in support of our youth outreach strategy.

This was discussed at HIF in November 2015, and approved by the Commissioner in March 2016.

According to Facebook, Pages “are for businesses, brands and organizations to share their stories and connect with people.... People who like your Page and their friends can get updates in News Feed.”¹ Pages can only be created and managed by an official representative of the business or organization.

Research suggests that Canadians are avid social media users, with Facebook as the most popular social network among Canadians. A Forum Research survey conducted in 2015 found that 59% of respondents had Facebook accounts, compared to 30% of Canadian respondents on LinkedIn, 25% on Twitter and 16% on Instagram. (According to Facebook's own research, 14 million Canadians check their Facebook

¹ *What is a Facebook Page?*, Facebook Help Centre, <https://www.facebook.com/help/174987089221178>

newsfeed every day.) Additionally, a study by the U.S.-based Pew Research Center study suggests that a large number of parents (66%) find parenting advice while looking at social media content.

Objectives

- To establish an OPC Facebook page devoted to and focused on communicating to Canadians in general, and in particular, communicating directly to parents with information on privacy issues and risks, and tips and strategies to mitigate those risks.

Additionally:

- to ensure that the OPC brand is properly reflected on our Facebook presence; and
- to ensure that our use of Facebook is compliant with our own internal privacy policies, the *Privacy Act* and relevant TBS guidance regarding federal government use of social media, and that our privacy practices with respect to our use of Facebook is consistent with the advice we have given other organizations.

Consultations

Following a discussion at HIF on the potential of expanding the Office's use of social media (beyond its blog, Twitter, YouTube and LinkedIn accounts) to include Facebook, HIF recommended that Communications consult with two DPAs currently using Facebook to better understand their considerations before establishing a presence on Facebook, specifically as it relates to the privacy of Facebook users who choose to follow these DPAs on Facebook, and any perceived conflicts of interest.

The OPC consulted with the UK's Information Commissioners' Office (ICO) and the Office of the Australian Information Commissioner (OAIC). Additionally, Policy & Research (P&R) assessed the risks, from a policy perspective, of our Office establishing a presence on Facebook.

Considerations

Perceived conflict of interest

There is the risk of a perceived conflict of interest, given that we have investigated Facebook's privacy practices in the past and could receive complaints where Facebook is named as the respondent. In its risk assessment, P&R determined that the risk that the Office could receive a complaint related to Facebook Pages is minimal as they consider such a complaint unlikely. As well, P&R concluded that there is minimal risk that the OPC might be seen to be endorsing a non-privacy compliant Facebook feature. (The risk assessment is contained in Officium document 7777-6-123918.)

In the consultations with the ICO and OAIC, both organizations concluded that there was minimal risk that their respective organizations might be seen to be endorsing a non-privacy compliant Facebook feature through their use of a Facebook page. However, both organizations drew the line at partnering

Officium 7777-6-146948

with Facebook in other ways – for example, like the OPC, who was also approached, both chose not to partner with Facebook to create a Data Privacy Day video that would be promoted on Facebook.

Facebook has been the subject of previous OPC investigations. Should Facebook become the subject of another investigation, Communications would consult with LSPRTA and PIPEDA Investigations to review this strategy and assess whether our use of Facebook as an organization would require any changes.

Privacy on social media:

Given our role, we must be cautious in our use of a new social media channel. This strategy is meant to address concerns with respect to user privacy and the OPC's use of Facebook. The approach was reviewed by the OPC's CPO, and discussed with the Office's Privacy Accountability Working Group (PAWG). It will be reviewed and approved by the Commissioner before the Page is launched.

The OPC has a formal process in place to determine if a PIA is necessary before launching a new project. If personal information is being collected, a PIA questionnaire must be completed. The questionnaire helps inform the CPO and PAWG in their consideration of whether a PIA is required. However, in this case, the OPC has confirmed with its CPO that, as with our approach to LinkedIn, a PIA is not required as the OPC, in its use of Facebook, will not be actively collecting any personal information, as defined in the *Privacy Act*, from its Facebook page. Communications has reviewed the questions in the PIA questionnaire and can confirm that it will not be collecting or using personal information in any of the ways identified in the questionnaire.

In our consultations with the ICO and the OAIC, they indicated they did not record or retain data about the people who follow/like their Facebook pages. Additional information on how the OPC would collect and use information via Facebook is in the section entitled *Collection and Use of Information Gathered on Facebook* in this document.

As part of the OPC's implementation plan, an OPC Facebook Privacy Notice would be drafted by our Office, explaining the OPC's collection and use of information gathered on Facebook, and a link to this notice would appear prominently on our page. Moreover, this notice would explain the third-party nature of the Facebook platform, note that Facebook users are bound by Facebook's Terms of Service and Privacy Policy, and encourage users to read the Terms of Service and Privacy Policy. For an example of what this notice could look like, please see our [LinkedIn](#), [Twitter](#) and [YouTube](#) Privacy Notices. Legal Services has reviewed these Privacy Notices and had no concerns. They will review the draft Facebook Privacy Notice and Comment Policy (discussed below) before the launch of the Page.

In its assessment, P&R also identified the risk that visitors to our Facebook page could post personal information (their own or someone else's) on our page. To mitigate this risk, P&R has recommended that we review all comments made to our page before posting, and delete or remove comments from our Page as appropriate. Facebook has the functionality to allow page administrators to do this. (However, we would note that [Facebook's privacy policy](#) indicates that these comments and/or information about these comments) are collected and retained, even after being removed from a page. We employ this same practice for comments readers make on our blog, and this practice would be outlined in our Facebook Comment Policy, explained further below in this document. A reminder about not posting personal information will also appear in the Privacy Notice.

Collection and Use of Information Gathered on Facebook

The OPC will not collect, record or retain any personal information, as defined in the *Privacy Act*, on Facebook.

Facebook provides aggregate data on page activity – e.g. number of likes, page visits and reach. (See screenshot below.) This data does not identify individual users. The OPC would use this aggregated information to evaluate and improve its use of Facebook as an outreach tool.



Comments made by Facebook users on our page or in response to our posts would be visible to other Facebook users. The amount of information that can be viewed about any Facebook user would depend on the privacy settings of that follower's account. This information will not be recorded or retained for any purpose. This will be made clear in our Privacy Notice, as has been done in the Privacy Notices for YouTube, LinkedIn and Twitter.

Staff with "administrator access" to the OPC's Facebook page will be limited to the Manager of Public Education and Outreach, the Director General of Communications, and one other communications advisor (as a back-up).

As per the OPC's [Privacy Notice](#), should the OPC become aware of comments that violate Canadian law, they will be deleted and such comments may be disclosed *to law enforcement authorities*.

Social media use policies and guidelines:

Officium 7777-6-146948

Treasury Board of Canada Secretariat has recently released a new Policy on Communications and Federal Identity, a supporting Directive on the Management of Communications and a Policy on Acceptable Network and Device Use. While the OPC is not subject to some parts of these policies and key portions of the directive, all Government of Canada institutions are encouraged to adopt the practices outlined in the policies and supporting directives, as appropriate. TBS' Directive on the Management of Communications encourages clear accountability for the management and coordination of departmental Web 2.0 initiatives and the development of strategies, plans and protocols for personnel on the use of Web 2.0. The OPC also has developed its own Acceptable Use of Electronic Networks Policy which defines the requirements for secure, ethical and appropriate use of OPC's electronic networks for business purposes.

ESDC and TBS have developed a draft Standard Privacy Impact Assessment (S-PIA) to determine the overall privacy risks associated with the use of official federal government social media accounts on a number of different platforms, including Facebook, and provide recommendations to mitigate these risks. The document has not yet been finalized nor has the OPC (Audit and Review) received it for review. As well, A&R has questioned whether the S-PIA should cover the use of so many different platforms. Note that the S-PIA covers a broad range of *activities* that departments could undertake using social media, including activities where, *unlike* the OPC's proposed use of one feature on Facebook, personal information may be collected. A&R will engage Policy and Research, as well as Communications, as appropriate, with respect to either further discussions relating to the S-PIA or other relevant PIAs on the use of social media by the GOC.

Reaching *other* audiences via Facebook:

At the moment, small businesses or other key OPC target audiences would not be viewed as the primary audience for use of this tool, as small businesses tend to use the Facebook platform to reach customers (as opposed to using the platform as a source for information about running a business). In the future, we could decide to broaden our use of Facebook to reach other audiences. Should this be contemplated, Communications will consult with others as appropriate.

Day-to-day management of the OPC Facebook page:

The OPC is currently active on LinkedIn and Twitter, and also has a YouTube account. Day-to-day management of the OPC Facebook page would be coordinated by the Manager, Public Education and Outreach of the OPC Communications Branch, who is already responsible for the OPC's other social media accounts.

Overall approach

This section covers strategic communications approach and tactics. It addresses:

- Approach to sharing and engaging
- Foundational elements to launch the page (OPC Facebook Comment Policy, OPC Facebook Privacy Notice, Posting guidelines / Service standards)

- Compliance with Government of Canada policies and guidelines (Identity, Official Languages, Accessibility, Publishing, Account configuration and compliance)
- Development of the Facebook Page (Development and branding, Account Verification)
- Ongoing management (Posting, Approval process, Daily management of Facebook page)
- Evaluation

Communicating and Engaging

The OPC plans to use Facebook as a platform for *sharing content* and *engaging with the public*.

With respect to *sharing content*, the OPC will:

- Communicate the OPC brand as a protector and promoter of privacy rights for all Canadians.
- Adopt a tone that is friendly, helpful, and approachable, keeping in mind that its target audience is adults with children and elderly parents; and
- Share existing and new OPC resources developed for individuals; inform the public of relevant news and announcements from our Office; and share relevant Facebook posts from other DPAs and other federal government organizations (e.g. Public Safety's Get Cyber Safe Facebook Page and Innovation, Science and Economic Development's Your Money Matters Facebook page).

With respect to *engaging the public*, in addition to the above, the OPC will:

- Be timely, accurate, clear, objective, responsive, respectful and fair in its communications with the public, as per our obligations under the Government of Canada's Policy on Communications and Federal Identity and the Government of Canada's Values and Ethics Code.
- Ensure our organizational use of Facebook is in compliance with internal and external guidelines, policies and legislation with respect to privacy; and
- Be transparent and open about our expectations and practices regarding users communicating with our Office via Facebook. (See the proposed Facebook Comment Policy below.)

Foundational elements

In order to launch the Page, the OPC must develop or establish a few key foundational pieces: a Comment Policy, Privacy Notice, Terms of Engagement and the Service Standard. Users can read more about these in our "Third-Party Social Media" section in the following link:

<https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/terms-and-conditions-of-use/#privacy>

OPC Facebook Comment Policy

Comments left on posts are made public on the Page automatically and immediately. A notification is also sent to the Administrators.

Administrators will review the comment and, if the comment meets any of the following conditions mentioned in the comment policy below, the comment will be hidden from the post. The Facebook Page will be monitored during business hours (Monday – Friday, 8:30am to 5:00 pm). Our Facebook Page will

indicate that the Page is monitored regularly during these hours. Comments may occasionally be reviewed outside of business hours (evenings, weekends and statutory holidays).

Comments left on our Page that meet any of the following conditions outlined in our Facebook Comment Policy may be edited or removed by the administrators of our Page. These will be reviewed on a case by case basis, consulting with Legal, Policy and others as appropriate. If a comment appears to add to the discussion but includes, for example, personal information, administrators may also choose to send a message to the individual user explaining why their comment has been removed. As a general practice, however, we will not notify users when we remove a comment.

The Comment Policy will be posted directly on our Facebook page. This draft Comment Policy, and the Privacy Notice below, have been approved by the Commissioner when this document was originally approved, August 15, 2016.). The Comment Policy and Privacy Notice were further reviewed and revised by Legal Services, September 8, 2016.).

Here is the proposed text for the Comment Policy:

All comments posted by Facebook users to the OPC's Facebook page, as well as messages sent to the OPC via Facebook will be reviewed by OPC staff with administrator rights to the page. Although we are not able to reply individually to all posts, comments and messages, they will be handled on a case-by-case basis and responded to when deemed appropriate.

The OPC cannot and does not provide advance rulings with respect to privacy issues on Facebook. We encourage you to contact the OPC's Information Centre with any privacy-related questions or concerns.

We reserve the right to edit or remove comments that meet any of the following conditions:

- *are contrary to the principles of the Canadian Charter of Rights and Freedoms;*
- *are racist, hateful, sexist, homophobic, defamatory, insulting, threatening, or otherwise discriminating or hurtful to an individual or group;*
- *put forward serious, unproven or inaccurate accusations against individuals or organizations;*
- *are aggressive, vulgar, indecent, rude, abusive, coarse, violent, obscene or pornographic in tone or content;*
- *are offensive, defamatory, disparaging or include defamatory statements to an individual or an organization;*
- *are not sent by the author and/or posted by anonymous or robot accounts;*
- *are put forward for phishing or spamming purposes;*
- *are written in a language other than English or French;*
- *are solicitations, advertisements, or endorsements of any financial, commercial or non-governmental agency;*
- *contain announcements from labour or political organizations;*
- *contain personal information about you or any other person;*
- *contain any names, products or services, logos, slogans, mascots, artwork, or promotion of any brand, product or service of any company or entity, or any material protected by copyright or trademarks;*
- *are unintelligible or irrelevant to the Page;*

- *encourage or suggest illegal activity;*
- *are repetitive or spamming of threads, and*
- *do not, in the moderators' opinion, add to the normal flow of the discussion.*

OPC Facebook Privacy Notice

The Privacy Notice will be posted directly on our Facebook page. Here is the proposed wording for our Privacy Notice, reviewed by Legal:

Facebook is a third-party service provider used by the Office of the Privacy Commissioner of Canada to communicate with the public. Facebook account holders who use the service are bound by Facebook's Terms of Service and Privacy Policy – this includes our Office, and individuals who communicate with our Office via Facebook. We encourage users to read Facebook's Terms of Service and Privacy Policy, as well as the Terms of Service and Privacy Policies for all social networking services they use.

Comments left by individuals on the OPC's Facebook Page can be read by anyone. Therefore, we strongly advise users not to post personal information – either their own, or the information of others – on our Facebook Page. As per our Facebook Comment Policy, the OPC reserves the right to remove any comments containing personal information.

The amount of information about a user that is available publicly depends on the user's privacy settings. The OPC reminds users to regularly check and adjust individual privacy settings as they may change over time.

Our Office may use information you provide on Facebook – including, but not limited to the personal opinions contained in your comments or messages to us – for statistical or analytical purposes.

Should you have any questions about your privacy rights as explained in this Privacy Notice, please contact our Chief Privacy Officer, who is also the Director of the Access to Information and Privacy Unit, through our toll-free line at 1-800-282-1376, or by postal mail at:

*30 Victoria St.
Gatineau, Quebec
K1A 1H3*

Posting guidelines / Service standards

Feedback and interaction is highly encouraged. All wall posts and comments, as well as email sent to the Facebook account will be read, and any emerging themes or helpful suggestions will be passed to the relevant people in the office.

Although we may not be able to reply individually to all private messages sent to our Facebook account, they will be handled on a case-by-case basis and responded to when deemed appropriate. The OPC will answer messages from the public in a timely manner and will be able to review its response time using the reporting tools in Facebook available to the administrators.

Officiium 7777-6-146948

Questions requiring a more elaborate response will be referred to the Information Centre. Individuals putting forward privacy complaints or concerns will be referred to the appropriate section of our website.

Reporters engaging us on Facebook will be asked to send questions to our Media Relations team.

Compliance with Government of Canada policies and guidelines

The following describes some of the key policies, guidelines and laws that can apply to government social media accounts and how we will ensure compliance with those that apply to the OPC.

Identity

The OPC is not subject to the standard visual requirements defined in the TBS Policy on Communications and Federal Identity. This means that we can use the OPC coat-of-arms to identify ourselves on Facebook (instead of the flag) or any image that we deem appropriate.

Official Languages

The OPC respects the Official Languages Act and is committed to ensuring that information products are available in both French and English, of equal quality.

OPC Communications will establish separate Facebook pages in English and in French, as per the approach recommended by the Government of Canada in its Policy on Communications and Federal Identity and in-line with our current use of Twitter.

Comments and questions that require a response will be answered in the official language of origin.

Users should be aware that some links direct users to sites of organizations or other entities that are not subject to the Official Languages Act and that these sources are only available in the language in which they are written. For example, we may choose to share a *New York Times* article only on our English page only, or a *La Presse* article only on our French page. We will aim to have the same number of posts shared in both languages whenever possible, however, there may be quiet days where only relevant posts in one language or the other.

Accessibility

The Government of Canada must comply with Web Content Accessibility Guidelines 2.0 (WCAG), which aims to make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these. Facebook allows for: compatibility with voiceover software for the visually impaired, captions to be added to videos (in .srt files) and full text to be accompanied with Infographics. Our office, in its commitment to achieving a high standard of accessibility, will ensure that our Facebook posts are accessible to visitors with disabilities and respect our Policy on Accommodating Clients with Disabilities.

Publishing

The OPC complies with section 6.3 of the policy on Procedures for Publishing, ensuring that when communications products are posted on third-party platforms, they are also available on Government of Canada websites. For example, our infographics will be posted on Facebook and will be available on our website as well.

Account configuration and compliance

We will comply with the Government of Canada's Technical specifications for social media accounts when creating our Facebook pages, ensuring that we are:

applying correct social media visual and text identifiers (requirement 2.1);	The Coat-of-arms or other relevant pictures will be used to identify the OPC on Facebook. The short usernames @PrivacyCanada and @ViePriveeCanada will be used to identify us quickly.
incorporating a link to the equivalent account in the other official language, if applicable (requirement 2.2);	A link will be featured in the "About" section on our Facebook pages, leading the user to the equivalent account in the other official language.
incorporating a link to the associated government web page (requirement 2.3); and	Our website is listed in the "About" section on our Facebook pages.
incorporating a social media notice (requirement 2.4)	Our social media notice will be posted directly on our Facebook page in a separate tab.

Development of the Facebook Page

Development and branding

As outlined in the critical path below, OPC Communications will establish separate Facebook pages in English and in French.

The Manager, Public Education and Outreach will lead the design of the page.

The branding will be the same for both accounts, with the OPC's coat of arms used as our identifying picture on Facebook.

We will use two short usernames to identify our pages. We recommend @PrivacyCanada and @ViePriveeCanada. These usernames allow users to easily find our page by typing it directly in Facebook's search bar – the shorter, the better for those typing on Facebook mobile.

Two mock pages have been prepared (English and French) and have been listed as unpublished, where only invited users can preview these pages, pre-launch.

Account Verification

Facebook can verify that a page is authentic for a business or organization. A gray checkmark is added beside the name of the page, which confirms for users that the page is truly managed by the identified organization.

This simple step could reassure Canadians that they are in fact dealing with the OPC on Facebook and not a fake group.

Most government departments have received verification from Facebook, such as Parks Canada, Veterans Ombudsman, Finance, Transport, Library and Archives Canada, Canadian Heritage, etc.

Verification also allows us to use the “Facebook Live” option to livestream our events.

Launch

The OPC’s Facebook page is expected to be launched in the fall of 2016. We will inform our provincial, territorial and international colleagues of the page in advance, and will encourage those with existing Facebook pages to help us promote it. We will also reach out to our stakeholders – including other federal government departments, NGOs and other associations – to inform them of our page and encourage them to “like” or share it in order to build followers.

More information can be found in the steps listed in the [Launch Plan](#).

Ongoing management

Posting

Communications will develop original content for posts from existing communications and outreach Materials, with an emphasis on those relating to the youth outreach strategy.

Posts can also be tied to special months or days such as Financial Literacy Month, Cybersecurity Awareness month and Pink Shirt day (anti-bullying promotion).

We will also share relevant materials from other organizations as appropriate. For example, we may share relevant material posted by other Government of Canada or data protection authorities’ Facebook accounts.

The number of posts will vary depending on how many appropriate and relevant materials for sharing are identified each week. We will aim to share with our followers one post every couple of days (for example, a news article or item created by another organization such as an international DPA or privacy advocacy organization), and to write one original OPC post on a weekly basis.

Prepared posts can be put into the Facebook publishing tool so that they may be scheduled to appear at a specific time, for example, on statutory holidays when the office is closed.

See **Annex A** for examples of posts.

Approval process

As with content developed for Twitter, all posts will be reviewed and approved by the Manager, Strategic Communications, and, in certain cases, may also involve approval by the DG, Communications and/or the Commissioner.

The Manager, Strategic Communications, will also review any articles and videos of interest from external sources before they are shared on the OPC page.

Daily management of Facebook page

As with content for our Twitter accounts, planned content for the OPC's Facebook page reside in a Facebook editorial calendar saved in Officium.

Below are the duties involved with managing both pages:

ACTIVITY	FREQUENCY
Answer questions posted on our wall and private messages. Provide generic answer to longer messages which will require a few days for a response	As needed
Create new content to be posted using existing resources from our website and our previous campaigns when possible	Weekly
Collection and reporting of metrics via the Communications Branch Quarterly Report Provide ideas/solutions to keep Facebook pages alive and useful	Quarterly
Change cover image	quarterly

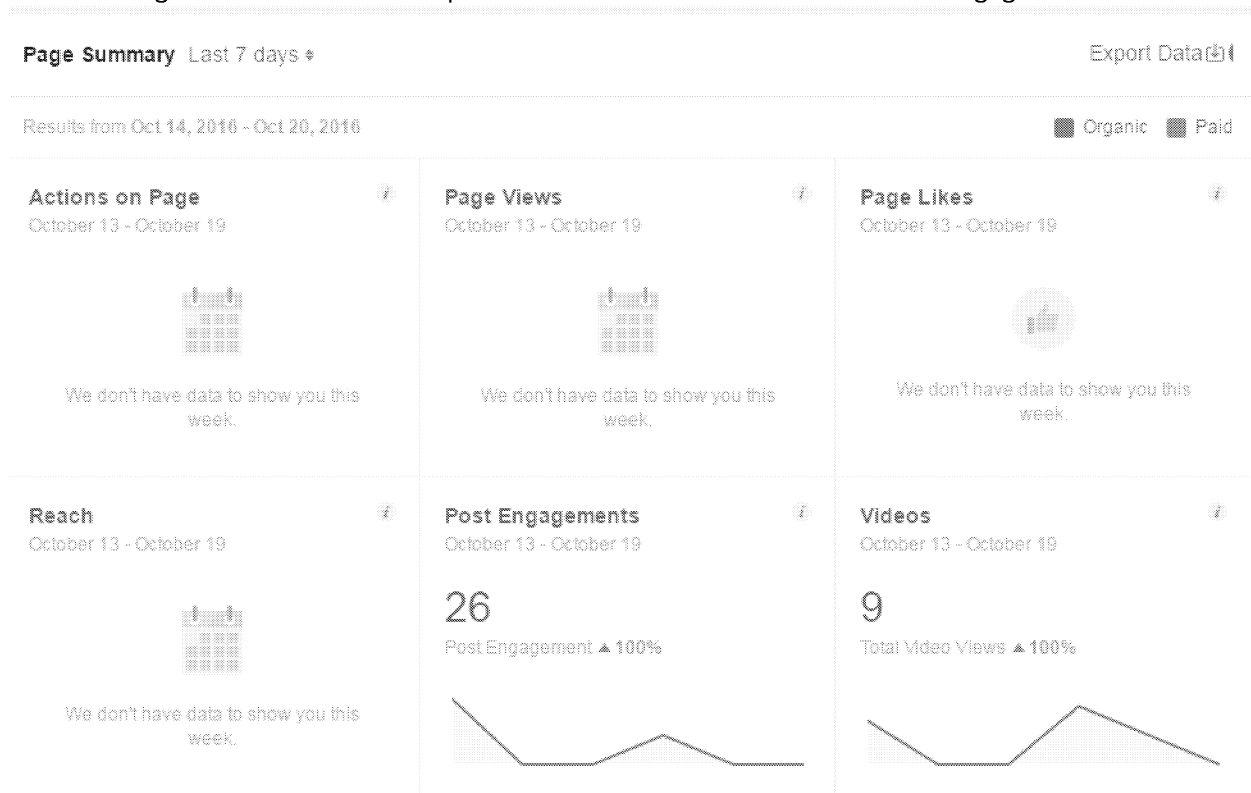
Evaluation

Measurement and Evaluation

As mentioned earlier, Facebook provides some basic analytics (anonymous and aggregated data) to owners of Facebook pages. The OPC will use this data to evaluate and improve its Facebook outreach strategy. This information will be included in the Communications Branch quarterly report, in which trends and statistics are included on web, media relations, social media, events and exhibits, and information requests.










Success in monitoring and responding to engagement (questions, comments, shares, etc.) will be measured through our response time and can also be measured by positive replies and likes on our responses. Sentiment will be tracked by taking a look at the type of likes (normal, Love, haha, Wow, sad and angry) tagged on our posts. As indicated in our Privacy Notice, we will not collect personal

information as part of our measurement and evaluation efforts. The Insights section provides useful data showing the total views for our posts and how well we have reached and engaged our audience:



Your 5 Most Recent Posts >

Reach: Organic / Paid
Post Clicks
Reactions, Comments & Shares

Published	Post	Type	Targeting	Reach	Engagement
10/20/2016 12:17 pm	 Once you put your personal information out there, you can't take it back. Watch as our video shows that it's almo			0	0
10/20/2016 12:10 pm	 Zoomer Show Lifestyle Expo for the 45+			0	0
10/20/2016 11:48 am	 Here's an interesting article to read: http://ottawacitizen.com/news/national/defence-watch/the-mystery-of-the-list			0	0

Critical path

ACTIVITY	TIMING / FREQUENCY
Develop FB strategy outlining objectives, target audiences, information management and privacy practices, and procedures for posting and engaging with the public (e.g. how are posts approved; who has access rights to post/review comments). Strategy will also outline launch strategy.	June 2016
Present FB strategy and invite comment from CPO, PAWG, Legal.	June-July 2016
Send FB strategy to Commissioner for review and approval	August 2016
Work with communications operations (Jana/Monique) to develop graphic elements for pages	August- September
Develop editorial calendar – ideally, first 2 months	August - September
Create pages (E/F); also complete form for verified account: https://www.facebook.com/help/contact/356341591197702	Jan 2017
Train backup(s) to post	Jan 2016
Create Facebook pages	Late 2016 – Jan 2017
Obtain approval from Communications and the Commissioner	Late 2016
Go live with our Facebook launch	Feb. 22, 2017

Annex A – Examples of posts

Sharing articles



Test test test
Published by Pierre-Luc Poisson (9) · 22 hrs · 🌐

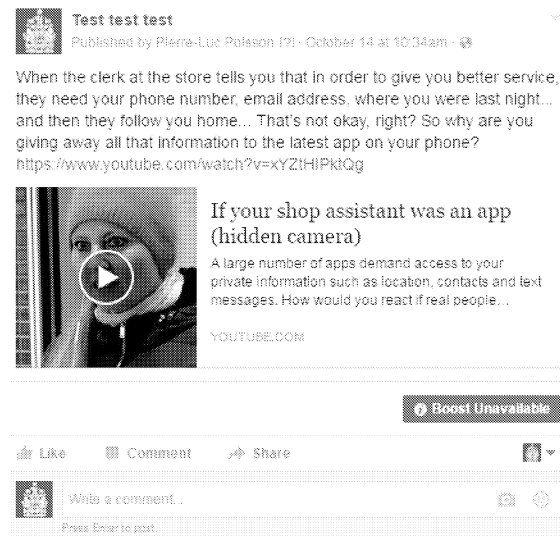
An interesting read – tell us what you think! <http://www.theatlantic.com/.../2.../10/babies-everywhere/502757/>



Giving Kids 'Veto Power' Over a Parent's Facebook Posts
All those Facebook photos are cute—but how are they affecting the kids?


THEATLANTIC.COM | BY ADRIENNE LAFRANCE

Sharing YouTube videos



Test test test
Published by Pierre-Luc Poisson (9) · October 14 at 10:34am · 🌐

When the clerk at the store tells you that in order to give you better service, they need your phone number, email address, where you were last night... and then they follow you home... That's not okay, right? So why are you giving away all that information to the latest app on your phone?
<https://www.youtube.com/watch?v=xYZtHlPkQg>




If your shop assistant was an app (hidden camera)
A large number of apps demand access to your private information such as location, contacts and text messages. How would you react if real people...

BOOST UNAVAILABLE

Like Comment Share

Write a comment...
Press Enter to post.

Facebook Note

 **Test test test**
Published by Pierre-Luc Poisson [?] · October 14 at 10:40am · 🌐



Mobile apps and protecting your personal info

Following the Denmark coffee shop story, here are our tips for protecting your personal information when downloading and using mobile apps: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/digital-devices/apps_info_201405/

[See More](#)

Video uploaded on our page

Test test test
Published by Pierre-Luc Poisson (7) · 3 mins · 🌐

Once you put your personal information out there, you can't take it back. Watch as our video shows that it's almost impossible to take back anything that you put online – much like getting the toothpaste back into the tube. Want to know more about protecting your online rep? Check out our website for more tips and tricks - <http://www.youthprivacy.ca>




1 View

👍 Like 💬 Comment ➦ Share

OPC post with link

Test test test
Published by Pierre-Luc Poisson (7) · October 14 at 10:32am · 🌐

Have you checked your privacy settings lately? Take a look at our ten tips so you can stop the fraudsters helping themselves to your identity: https://www.priv.gc.ca/.../id.../identity-theft/id_info_201303/



10 Tips for preventing identity theft - Office of the Privacy Commissioner of Canada
Get some everyday tips for reducing your risk of identity theft.
PRIV.GC.CA

👍 Like 💬 Comment ➦ Share

Last updated: February 13, 2016

Facebook Page Launch Plan

The Communications Branch proposes to launch the OPC's new Facebook Page February 22nd.

This document describes key steps required ahead of the launch; sets out the first seven proposed posts for the new Page; and describes how key stakeholders would be advised of the launch and how the OPC would work to build its network of followers.

Key steps:

1. Completion of foundational elements

Both Facebook pages (English and French) have been created. The Comment Policy and Privacy Notice are available for the user directly on our Facebook page, on the right-hand side menu. The OPC Privacy Policy from our website is also directly highlighted on the Facebook pages.

2. Verification

We will verify both of our pages with Facebook in order to appear as a legitimate organization and to enable the Facebook Live feature. Facebook will verify our pages as soon as they are live. A checkmark is added beside the name of the page, which confirms for users that the page is truly managed by the identified organization.

3. Content development

Our plan is to post one or two items per week.

Here are the seven proposed posts to start:

1. Introduction

Focusing on kids and parents:

2. Pointer to youth resources
3. DYI House rules
4. Twelve quick privacy tips for parents

Posts of general interest:

5. Identity Theft (Income tax season)
6. Do Not Call List
7. Managing App Permissions (Denmark Bakery video)

Please refer to [OPC Facebook Schedule](#) for the full text.

4. Page promotion / building followers

We will work to build visibility for the new page right from the day of the launch. Steps to encourage traffic will include sending email notices to stakeholders and FPT; promoting the page via our other social media channels and GCConnex; and encouraging other organizations to “Like” the page. We will also promote on our website.

Announcement and web promo

On the day of launch, we would post a brief Announcement on our website.

We will also add a Facebook button on our website in the bottom right corner under the section “Stay Connected,” along with the other social media links.

We would include a slider to promote the Facebook page on our website homepage during the first few weeks after the launch.

Advising staff

- To ensure OPC staff are aware of the FB page and its purpose, an email will be sent to all staff by the DG Comms, with similar messaging (touching on employee privacy issues) to the message used when the LinkedIn page was announced, given that some staff may choose to “like” or “follow” the OPC FB page.

Advising stakeholders

- An email from the DG, Communications will be sent through the FPT listserv to let organizations know that the OPC is now on Facebook.
- An email will be sent to privacy advocates (Media Smarts, Digital Tattoo) and our broader stakeholder list, and any other relevant listservs, from the DG, Communications to let them know that the OPC is now on Facebook (as we did when we launched the new website).

Use of other social media channels

Our Facebook page will be promoted on Twitter, on LinkedIn, on GCConnex, on Facebook by liking pages from other organizations and by email internally and externally.

Here is a brief explanation for each medium to be used:

Twitter, LinkedIn

We can use these two messages on Twitter and LinkedIn with the OPC’s accounts to reach our followers:

- We are now on Facebook! Come check out our page at <https://www.facebook.com/PrivCanada/>

- Nous sommes désormais sur Facebook! Venez voir notre page au <https://www.facebook.com/ViePriveeCanada>
- Come see us on Facebook, we have info for parents and youth on privacy rights and how to better protect personal information <https://www.facebook.com/PrivCanada/>
- Venez nous voir sur Facebook pour des infos aux parents et jeunes sur droits à la vie privée et protection des renseignements personnels <https://www.facebook.com/ViePriveeCanada>

GCconnex

GCconnex is an effective way to communicate to Government of Canada employees that we are on Facebook. The OPC does not currently have a group page on GCconnex, but communications officers can use their own accounts to send out two messages with this wording on The Wire, GCconnex's own microblog, which behaves much like Twitter.

We will display these messages on GCConnex's Wire:

- We are now on Facebook! Come check out our page at <https://www.facebook.com/PrivCanada/>
- Nous sommes désormais sur Facebook! Venez voir notre page au <https://www.facebook.com/ViePriveeCanada>

Liking other pages

In order to build followers, the OPC will "Like" pages from other organizations, and send a message to these organizations to be liked back: "Hello, we're now on Facebook! We've liked your page and hope you'll consider liking ours. Thanks!"

We will do the same with our French page, using this message: "Bonjour, nous sommes désormais sur Facebook! Nous avons choisi d'aimer votre page et nous espérons que vous choisirez d'aimer la nôtre"

The following is a list of organizations we will Like, to start:

Government Departments – Federal and Provincial

- Senate
- Information Commissioner
- Financial Consumer Agency of Canada (@FCACan and @ACFCan)
- Veterans Ombudsman (@VeteransOmbudsman and @OmbudsmanVeterans)
- Senate (@SenCanada)
- Information Commissioner (@OICCANADA)
- Official Languages Commissioner (@officiallanguages and @languesofficielles)
- Justice (@JusticeCanadaEN and @JusticeCanadaFr)
- Parks Canada (@ParksCanada and @ParcsCanada)
- Canadian Heritage (@CdnHeritage and @Patrimoinecdn)
- National Capital Commission (@NationalCapitalCommission and @CommissionDeLaCapitaleNationale)

- Information and Privacy Commissioner of Ontario (@IPCOntario)
- Healthy Canadians (@HealthyCdns and @CanenSante)
- Get Cyber Safe (@GetCyberSafe and @Pensezcybersecurite)
- Your Money Matters (@YourMoneyMatters and @QuestionsdargentCanada)

External Organizations

- Office of the Australian Information Commissioner (@OAIcGov)
- Federal Trade Commission (@federaltradecommission)
- Commission Nationale de l'Informatique et des Libertés (@CNIL)
- Information Commissioner's Office (@ICONews)
- Canadian Centre for Child Protection
- MediaSmarts (@MediaSmarts and @HabiloMedias)
- Digital Tattoo (@digitaltattoo)
- Éducaloi (@educaloi)

Critical path before and during launch day

ACTIVITY	DATE / FREQUENCY	RESPONSIBILITY
Demo for Commissioner, proceed with steps for approval by Commissioner	Week of February 13	Valerie/AMH/ P-L/AMC
For Web: Ask to prepare the mention of Facebook on our webpage <u>Terms and conditions of use</u> (add to the list of social media platforms in Third-Party Social Media) on launch day Ask to add the Facebook button in "Stay Connected" on our website on launch day Prepare home page slider Prepare Announcement	Week of February 13	Pierre-Luc to liaise with Heather and Monique
Remind Facebook to verify pages on launch date	February 21	P-L
Circulate an email internally to let employees know about the launch	February 21	AMH
LAUNCH DAY	February 22	

<ul style="list-style-type: none">• Put first post on our wall – Introductory post• Emails from Anne-Marie Hayden: stakeholders, FPT through ListServ• Post Announcement about Facebook launch on OPC website. Alert staff of announcement via email.• Promote our Facebook Launch on Twitter and LinkedIn• Like pages from other organizations and ask to be Liked back• For web: display item on Terms and conditions of use, add Facebook button.• Post to GCConnex• Facebook verifies our pages, adds checkmark		P-L AMH MF AMC P-L MF P-L P-L
--	--	--