BILL C-30 AND INTERNET PRIVACY

Introduction

Focus
After Prime Minister Stephen Harper's Conservative government was re-elected in 2011, it decided to resurrect a bill that would give police the power to access subscriber information from Internet providers without a warrant. This *News in Review* story looks at the controversy surrounding this legislation, known as Bill C-30.

The government calls it "lawful access." Opponents call it an unprecedented invasion of privacy. Bill C-30 set off a national debate regarding what information should and should not be legally protected from the curious eyes of the authorities.

When the Conservatives were re-elected on May 2, 2011, this time with a majority, the proposed legislation giving the police easier access to Internet subscriber information was back on the table.

It fell to Public Safety Minster Vic Toews to introduce the bill in the House of Commons. Put simply: Bill C-30 would give the police the right to access subscriber information from Internet service providers (ISPs) without a warrant while also compelling those providers to build in a surveillance network for police to monitor alleged criminal activities taking place online. The monitoring itself would require a warrant.

While Toews felt the bill was reasonable and fair, opponents responded that the legislation was unnecessary and too far-reaching. After all, ISPs had already been accommodating close to 95 per cent of all police requests for subscriber information. When an opposition critic challenged the minister in the House, Toews responded that the member could "either stand with us or with the child pornographers." This set off a firestorm of debate that eventually forced Toews and the Conservatives into a major retreat. Opponents knew they had scored points when the government volunteered to send the bill to committee after second reading for amendments and revisions—a step usually skipped because majority governments can pass whatever legislation they want without having to entertain additional debate.

Meanwhile, other opponents took Toews to task. Local and national news media challenged the government's disregard for privacy, with most pointing out that the Conservatives scrapped the long-gun registry and the long-form census in the interests of public privacy and now they were introducing legislation that was much more intrusive. The hacker group Anonymous posted a YouTube video threatening to invade the privacy of Toews, and several Twitter feeds streamed personal information about him. One Twitter account, called #vikileaks30, turned out to be the work of a Liberal staffer who tweeted details of Toews's divorce. This individual was eventually identified and forced to resign.

The irony of the situation is that Bill C-30 probably would have passed virtually unnoticed if Toews had not cast anyone who opposed his legislation as an ally of child pornographers. Privacy advocates owe a debt of gratitude to the Public Safety Minister for his statements. By April 2012, it appeared that the final version of Bill C-30 will look quite different from the one Toews initially presented to the House.

To Consider

1. What is "lawful access" and how does it apply to the Internet?
2. Outline the main goals of Bill C-30.
3. Why did the comments of Public Safety Minister Vic Toews in the House of Commons set off a national debate on privacy?
4. Why do privacy advocates owe a debt of gratitude to Public Safety Minister Toews for his statement while defending Bill C-30 in the House of Commons?

BILL C-30 AND INTERNET PRIVACY

Video Review

Did you know . . .
A warrant is a document issued by a judge that gives the police the power to conduct surveillance, arrest, and/or search the property of suspected criminals.

Pre-viewing Activity

With a partner or in a small group discuss and respond to the following. The law enforcement community is concerned about criminal activity occurring online. It claims it needs more power to investigate certain individuals suspected of involvement in such activities so they can be quickly identified and brought to justice. Should the police be given the opportunity to gather information on people suspected of criminal activity without a warrant issued by a judge? Should they be allowed to monitor a suspect's online activity without a warrant?

Viewing Questions

As you watch the video, respond to the questions in the spaces provided.

1. What is Bill C-30? Why is it so controversial?

2. What is the government hoping to accomplish with Bill C-30?

3. How many people signed an online petition protesting Bill C-30? Did this have any impact on the government's decision to move ahead with the bill?

4. a) What information could the authorities access under Bill C-30?

   b) What justification would authorities need in order to access the information?

   c) At what point would a person be notified that he or she was the subject of a police investigation?

5. a) Why do some critics believe that Bill C-30 will turn Internet service providers into government spies?

b) What does Public Safety Minister Vic Toews think of this concern?

6. What comments did Vic Toews make to cause outrage in the House of Commons and across Canada?

7. How much do experts estimate surveillance technologies will cost Canadians if Bill C-30 passes?

8. What upsets Open Media's Steve Anderson about Bill C-30?

9. a) What was the online reaction to Bill C-30?

b) What happened to the Ontario Association of Chiefs of Police website?

10. a) What did the *Ottawa Citizen* discover about the Vikileaks Twitter feed?

b) Why was this development embarrassing to the Liberal Party?

c) What happened to the creator of Vikileaks?

Post-viewing Questions

1. After watching the video, revisit your responses in the Pre-viewing Activity. Did watching the video help you respond to the questions in greater depth? In what way?

2. In the introduction to the video, *New in Review* host Michael Serapio notes that, whether we like it or not, our personal information is being tracked just about every time we turn on a computer. Both Facebook and Google target advertising based on our online surfing, with Facebook taking the extra step of using your age, birthday, and "likes" to target its advertising. All this is done with little protest from the public. However, when the government introduced Bill C-30, people were vocal about the potential intrusion into their personal privacy. How do you explain the fact that Facebook and Google can track online behaviour without much protest, but when the government announces something similar there is a great deal of controversy?

BILL C-30 AND INTERNET PRIVACY

YV *What is Bill C-30?*

Did you know . . .
An Internet protocol (IP) address is a unique number assigned to a computer working on a network that functions about the same way as a home address. The IP address identifies the Internet subscriber and acts as a point of reference as people send and receive data to him/her over the Internet.

Before Reading

How would you feel if you knew the police had the right to force your Internet service provider (ISP) to provide your name, home address, e-mail address, phone number, mobile number, and ISP address without a warrant issued by the courts? Would you consider this an invasion of your privacy or just a case of the police doing their job? What potential benefits would there be to giving the police these powers? How could such powers be abused? With a partner, respond to these questions before reading the following section, and then revisit your responses after you have finished reading it.

Lawful Access

For over a decade, members of Parliament have been trying to draft legislation to give police more power to investigate and charge people who commit crimes via the Internet. A key component of this type of legislation is so-called "lawful access," which would give police access to information without a judicial warrant. Governments have been trying to introduce a bill concerning lawful access since the late 1990s.

A good time to pass a bill?

The latest edition of the lawful access legislation came in the form of Bill C-30. At first, the Conservatives tried to push the legislation through in an omnibus bill that contained a cluster of Conservative policies that died on the Order Paper prior to the last election. Eventually the lawful access bill was removed from the omnibus package, and Public Safety Minister Vic Toews presented the stand-alone bill in the House of Commons. Toews had two things on his side: one, many tech-savvy Canadians understood that it was just a matter of time before the Internet was subject to more policing and, two, many Canadians held fairly relaxed views regarding their personal privacy. The online behaviour of many people on Facebook and Google—where privacy is routinely surrendered—was clear evidence of this trend. These two things created a climate where Canadians implicitly understood the rapid growth and development of Internet technologies and indicated a willingness to concede their right to privacy if this meant a more pleasant Web surfing experience. Even with various privacy advocates expressing their concerns to the media, most Canadians did not seem to be paying much attention to Bill C-30.

Critical Error

But Toews made a critical error shortly after introducing the bill. When challenged by a fellow member of Parliament about the validity of the bill, Toews told the member that he could "either stand with us or with the child pornographers." The provocative statement set off a public outcry. Suddenly all eyes turned to Bill C-30—and people were shocked to see the wide-ranging powers the government was trying to hand over to the police.

In its original form, Bill C-30 would have given the police access to a great deal of private subscriber information held by ISPs—including a person's name, address, phone number, mobile number, and IP address—without a warrant. It also would give the police broad surveillance powers to monitor criminal activities in real time with the mandatory co-operation of the ISPs. The bill continued to describe the hardware upgrades ISPs would need to purchase to improve police surveillance powers

FYI
The RCMP made more than 28 000 requests for customer names and addresses from ISPs in 2010. The customers would never have known that a request was made about them.

while also providing law enforcement authorities with the opportunity to install their own hardware on the network of any ISP if they felt such a move to be necessary.

The Critics

Critics of the bill suddenly had a voice after Toews's inopportune and controversial comment. The main thrust of the criticism was: if police want to investigate Canadians—get a warrant! All opposition parties, and even a few Conservatives, took up this refrain.

Meanwhile, many Canadians were shocked to learn that ISPs had been voluntarily surrendering personal information (mainly names, addresses, phone numbers and IP addresses) to police for years. In fact one report claimed that ISPs accommodated police requests 95 per cent of the time, so a climate of warrantless access already existed.

You'll be paying

Canadians were also worried about the surveillance technology costs associated with Bill C-30. Essentially, the bill would create an infrastructure for police to access subscriber information without a warrant and to monitor subscribers with a warrant. Currently, no such infrastructure exists, and experts estimate the cost would be a minimum of $80-million. This cost would either be assumed by the taxpayer or the Internet subscriber. In other words, either way, Canadians would pay.

Future Misuse?

Finally, privacy advocates were worried that, once legal access legislation was passed, the opportunity for misuse of Internet subscriber information would follow. Since basic information could be accessed without a warrant, what would stop the authorities from randomly looking into the private information of some Internet users? And since the police would have the power to access certain information without a warrant, those subject to an investigation would never know they had been investigated.

Back to Committee

The torrent of controversy and concern was so intense that the government had to retreat on Bill C-30. The bill was sent back to committee after second reading (a step rarely taken by majority governments) for revisions and amendments. Critics hope the revised version of the legislation would clearly define what the police could and could not investigate when it comes to the online lives of Canadians.

To Consider

1. With a partner, revisit your responses to the questions asked in the Before Reading instructions above. How did reading this section influence your responses to these questions?

2. Why did some people support Bill C-30?

3. What happened that made the bill an issue of concern to many Canadians?

4. What surveillance powers would Bill C-30 give to police? Who would pay for the surveillance technology? Do you agree with this? Why or why not?

5. Bill C-30 was so controversial that the government decided to send the bill back to committee after second reading for amendments and revisions. From what you have read, what were the main flaws of the bill? Which of its terms were in need of major revisions?

BILL C-30 AND INTERNET PRIVACY

YV *Fixing Bill C-30*

Reading Prompt

The public debate over the government's controversial online surveillance bill became so intense that the Conservatives took the very rare step of sending the bill back to committee for debate and review after second reading in the House of Commons. To critics of the bill this was a small victory that indicated that the government was aware that Bill C-30 constituted a major breach in the online privacy of Canadians. Keep this in mind as you read Michael Geist's recommendations for fixing Bill C-30.

Professor Michael Geist and the Bill C-30 Fix

If you do any serious research about Canadian law and the Internet, you are bound to come across the name Michael Geist. The University of Ottawa professor is the Canada Research Chair in Internet and E-commerce Law for the university and is a regular contributor to the public debate on issues dealing with the Internet. Therefore, it was no surprise that, when Bill C-30 was introduced in the House of Commons, Geist had a great deal to say—and most of it wasn't very flattering for the Conservative government and Bill C-30.

From the very start, Geist pointed out that police had consistently failed to demonstrate the need for the lawful access provisions found in Bill C-30. Canadian Privacy Commissioner Jennifer Stoddart reinforced this point when she said: "Canadian authorities have yet to provide the public with evidence to suggest that CSIS or Canadian police cannot perform their duties under the current regime." The current regime calls for police to obtain a warrant if they want to access and monitor the online behaviour of people they suspect of conducting criminal activities on the Internet.

As the controversy over Bill C-30 forced the legislation back to committee for debate and revision, Geist proposed 12 steps to fix the online surveillance bill. The following is a simplified summary of his ideas.

The Bill C-30 Fix

1. Provide Canadians with evidence that law enforcement needs lawful access legislation. The existing warrant-based system seems to be working reasonably well. Why change it in favour of a new system that might be more prone to abuse?

2. Create a proper warrant for investigating Internet crime. Warrantless access to information is the most contentious aspect of the bill. While police complain that some warrants do not effectively cover the type of information they are looking for, Geist argues that a new kind of warrant could be created to allow police timely access to the information they need.

3. Report warrantless disclosure of subscriber information by ISPs. While Bill C-30 would create a reporting system for warrantless sharing of information, Geist worries that the voluntary system that already sees police requests honoured 95 per cent of the time already constitutes a major breach of privacy. However, if the legislation is pushed through, proper reporting of warrantless disclosure needs to take place.

4. Remove the disclosure gag order. Bill C-30 would prohibit ISPs from informing their subscribers that their information was disclosed to the police. Geist argues that informing subscribers is not unreasonable in many cases and that the government should work with ISPs to determine when disclosure would be appropriate.

5. Scrap voluntary warrantless sharing of information. Bill C-30 opens the door for police to ask ISPs to share subscriber e-mail and Web surfing histories. The fear is that the voluntary sharing of information that is already occurring might go one step further, with ISPs giving police information that should be the subject of a judicial warrant. Some sections of the bill also encourage this kind of sharing and provide immunity to ISPs for their co-operation. Geist thinks the legislation needs to do away with voluntary information sharing.

6. Clarify the extent to which surveillance technology will be used. The section dealing with surveillance is vague enough for law enforcement agencies and the government to take substantial liberties when it comes to looking into the online behaviour of Canadians. In fact, Bill C-30 gives the government the right to compel ISPs to install certain surveillance software and hardware at their expense as well as equipment provided by the government itself. The language of the bill needs to be much more specific when it comes to what constitutes legitimate surveillance and how surveillance technologies will be used.

7. Take another look at the burden being placed on ISPs. The government is asking ISPs to dramatically change their networks to make surveillance easier for law enforcement. It also goes to great lengths to outline the reporting process that ISPs will have to complete to demonstrate to the government that they are fulfilling the surveillance wishes of the police. In essence, the language of the bill makes the ISPs look more like an agent of the state than a private company working in the interests of its customers.

8. Create accountability in the law. Geist would like to see a much more comprehensive system of reporting so that confidential watchdogs (like the privacy commissioner) can make sure that the surveillance system is not being abused by law enforcement.

9. Limit the law to serious crimes. Determine which crimes are subject to surveillance and which are not. An open-ended bill could lead to simple snooping by police. Vic Toews and the Conservatives claimed that the bill was designed to lead to the arrest and conviction of people involved in child pornography. This is certainly an example of a serious crime.

10. Let Canadians know how much it is going to cost. Initial estimates put the surveillance technology and system upgrades at $80-million. Geist claims that the cost will be much higher given the infrastructure and bureaucratic changes the legislation will mandate both at the government level and with the ISPs. If the real cost is going to be over $80-million, Canadians need to know how this will affect their taxes if the government is footing the bill or how much more they will pay for their Internet if they are downloading the costs onto the ISPs.

11. Fill in the blanks. Geist encourages those drafting Bill C-30 to fully disclose the language that will appear in the final version of the bill. He feels that there are unspecified regulations

that can be shaped and used in a variety of ways that might lead to inappropriate surveillance by law enforcement.

12. Improve Canada's privacy laws. If the government wants lawful access legislation, they should also agree to update Canada's privacy laws to clearly define what privacy means in the digital age.

Source: "How to fix Canada's online surveillance bill: A 12-step to-do list," www.michaelgeist.ca/content/view/6339/125/. For a more comprehensive understanding of the Geist's perspective on this issue, visit www.michaelgeist.ca.

To Consider

1. Based on Geist's recommendations, do you think Bill C-30 can be reworked into something Canadians accept as not constituting an unreasonable intrusion on their personal privacy?

2. Is there really a need for the kind of surveillance the police are looking to obtain when it comes to Internet crime?

3. Does Bill C-30 infringe on the rights of ISPs to operate a private business?

BILL C-30 AND INTERNET PRIVACY

VI *The Vikileaks Affair*

Before Reading

Imagine that the government was trying to pass legislation that you disagreed with on principle. Would it be acceptable for you to show your opposition by setting up a website condemning the government's action? Would it be acceptable for you to make the website anonymous so that no one knew that the site was created by you? Would it be acceptable for you to post personal and private information about cabinet ministers in an effort to embarrass or humiliate them as part of your campaign against the government's legislation? With a partner, respond to these questions and revisit your responses to them after reading this section.

When Public Safety Minister Vic Toews responded to an opposition critic's concerns about Bill C-30 by saying "he can either stand with us or with the child pornographers," he set off an explosion of outrage. The media were quick to attack Toews for his incendiary rhetoric, with more than a few journalists using the minister's "child pornographers" analogy to add fuel to the fire of their argument.

While a great deal of ink was spilled in opposition to Bill C-30, it was the Internet where the most damaging attacks on the legislation appeared, which makes sense given the fact that the bill dealt with surveillance of people's online activity. Websites surfaced almost immediately decrying Toews and the Conservatives for threatening to invade the online private lives of all Canadians. The hacker group Anonymous posted a YouTube video threatening to release private information about Vic Toews if he didn't withdraw Bill C-30. It also hacked the website of the Ontario Association of Chiefs of Police after the organization released a statement in support of Toews and the bill. But the most damaging attack of all came from a Twitter account called #vikileaks30.

The Vikileaks Twitter account started with the provocative declaration, "Vic wants to know about you. Let's get to know Vic." What followed were intimate details of Vic Toews's divorce proceedings. While the information was a matter of public record, many questioned the ethical legitimacy of such a personal attack that was not related to Bill C-30.

As Vikileaks posts streamed on, a campaign to catch the author ensued. Toews's colleague John Baird initially blamed the NDP. But after a few days it became clear that catching the tweeter would be no easy task and any accusation without some kind of proof would do nothing but inflame the situation. That is until the *Ottawa Citizen* set up an online sting. A reporter sent #vikileaks30 an e-mail with a link to another website. The author of Vikileaks took the bait and clicked on the link. This allowed the *Citizen* reporter to isolate the IP address of the computer the author was using and, after a bit more digging, determine that the address belonged to a House of Commons computer. Shortly after the *Citizen* reported its discovery, Vikileaks went silent.

While the Twitter account lay dormant, the hunt for the Vikileaks author ramped up. The Speaker of the House of Commons launched an investigation into the account. The computer could be identified, but not the author. Finally, with the pressure of the investigation

mounting, and potential damage to his political masters in the balance, Liberal staffer Adam Carroll informed the party's interim leader Bob Rae that he was the author of the feed and promptly resigned from his job as a researcher.

A humbled Bob Rae apologized to Toews and the House of Commons for the ethical breach. He said that personal attacks have no place in public life. The message was clear: If an opposition member wants to criticize a public figure from the government, he or she needs to focus on policies and issues and avoid resorting to mudslinging and personal gossip.

While Bill C-30 was sent back to committee after second reading, politicians wondered if they had entered a new era in public life. Suddenly the prospect of making enemies for supporting policy initiatives (a routine hazard in politics) was being combined with potential public humiliation on the Internet.

To Consider

1. With your partner, revisit your responses to the questions in the Before Reading instructions above. How did reading this section influence your responses?

2. How did the online community react to Bill C-30?

3. What is Vikileaks?

4. Do you think Vikileaks crossed the line from an ethical standpoint?

5. If a group like Anonymous can hack into large, secure websites, what can prevent it from hacking into the surveillance network that Bill C-30 is asking ISPs to create? In other words, could the proposed surveillance network make the private information of Canadians even more vulnerable to the hacking skills of groups like Anonymous?

BILL C-30 AND INTERNET PRIVACY

Activity: A Parliamentary Committee Hearing

Your Task

For this activity you will prepare and present a debate regarding Bill C-30 and any amendments that might be made to it as it might occur during a session of the parliamentary committee investigating the bill. Sending any proposed piece of legislation to such committees for detailed review after it has been introduced in Parliament is a normal part of the procedure involved in enacting a new law.

Resources

Use the information included in this *News in Review* story to prepare for your debate. You may also wish to consult the following link from the CBC website and other links related to this story: "Online surveillance critics point to foreign experience," www.cbc.ca/news/canada/calgary/story/2012/02/21/pol-c30-surveillance-caution.html.

Background

The Harper government conceded that more work needed to be done before Bill C-30 could be passed. On the one hand, the government maintained its commitment to giving law enforcement authorities more power to investigate crimes occurring on the Internet. On the other, privacy advocates were able to demonstrate to the government that some information should remain private and that obtaining a warrant prior to an investigation was not an unreasonable requirement for police. Based on these two perspectives, the government agreed to send the bill back to committee for more debate and legislative amendments before reintroducing it to Parliament. Your task is to assume the role of a representative of one of the political parties at the committee meeting arguing for one of the perspectives indicated above.

Process

1. Form a group of four people. Each person in the group will pretend to be a member of one of the following political parties:

   Conservative — in favour of Bill C-30

   Liberal — opposed to Bill C-30 after first reading

   NDP — opposed to Bill C-30 after first reading

   Green — opposed to Bill C-30 after first reading

2. Conduct research into the details surrounding Bill C-30. Once you feel you have gained enough information to present your viewpoint, stage a mock committee meeting where you debate the strengths and weaknesses of the bill. The Conservative group member will chair the meeting.

3. The meeting will follow this agenda:

   a) Summary with briefing notes for each party

   b) Conservative perspective — 5 minutes
   You want to obtain information from Internet service providers (ISPs) without a warrant. Meanwhile monitoring online activity will only be possible with a warrant. You also want ISPs to install $80-million in

software and hardware upgrades so you can monitor online criminal activity in real time and with greater ease.

c) NDP, Liberal and Green perspectives — 5 minutes each
Collectively you oppose the need to put warrantless access to information into law since i) this constitutes an invasion of an Internet user's privacy and ii) ISPs are already honouring police requests for user information 95 per cent of the time. You also believe that the $80-million surveillance technology upgrade will mean either higher taxes for Canadians (if the government pays for the equipment) or higher Internet bills (if the ISPs pay for the equipment).

d) Challenge
Each party will have three minutes to challenge the perspectives put forward by any of the other parties.

e) Amendments
Hold a roundtable discussion of perspectives and challenges. Take the existing bill and decide which components to keep and which to discard. This should take around 15 minutes to complete.

4. The New Bill C-30: As a group, prepare a summary of your revised bill as you would like to see it presented to the House of Commons. Hand your new Bill C-30 in to your teacher or present it to your classmates. As a class, evaluate the new Bill C-30 to determine whether it addresses the concerns that were made at the time when the government introduced the original version of the bill in Parliament.