Communications networks have been the key to the social cohesion, political unity and economic development of Canada as a nation. Both burdened and blessed by our vast territory, generations of Canadians have trusted that their personal messages would be quickly and confidentially carried by the technology of the day — horse, telegraph, trans-Atlantic cable, microwave and satellite – to their destination.

These networks have been subject to oversight by state and public bodies for many years. As a result, network providers have been subject to legislation, regulations and guidelines addressing factors including regional service levels, the production of domestic content, competitive positioning within the domestic marketplace, and the protection of personal information. Similar expectations, and regimes, exist elsewhere around the world.

In 2007 and 2008, telecommunications pioneers, consumer activists and privacy advocates in the United Kingdom and the United States were disturbed to discover that a few telecommunications providers were participating in experiments to test the use of a network management tool in targeting marketing campaigns and advertisements at specific individuals.

This tool, deep packet inspection (DPI), allows network providers to peer into the digital packets that compose a message or transmission over a network. DPI has been used for several years to maintain the integrity and security of networks, searching for signs of protocol non-compliance, viruses, malicious code, SPAM and other threats.

DPI technology raises privacy concerns because it can involve the inspection of information sent from one end user to another. In other words, DPI technology has the capability to look into the content of messages sent over the Internet – enabling third parties to draw inferences about users' personal lives, interests, purchasing habits and other activities.

The technology has the potential to give ISPs and other organizations widespread access to vast amounts of personal information sent over the Internet for:

- Targeted advertising based on users' behaviour while browsing the Internet:
- Scanning network traffic for undesirable or unlawful content, such as unlicensed distribution of copyright material or dissemination of hateful or obscene materials;
- Capturing and recording packets as part of surveillance for national security and other crime investigation purposes; and
- Monitoring traffic to measure network performance, and plan for future facilities investments.

In light of privacy concerns prompted by this application of DPI, the Office of the Privacy Commissioner (OPC) wanted to create an opportunity for active public discussion of the issue – not only with respect to the impact of DPI technology on personal privacy, but about the broader importance of protecting personal information on the Internet. This project was the result.

In the summer and fall of 2008, the Research, Education and Outreach Branch of the OPC contacted leading academics and professionals working in telecommunications, law, privacy, philosophy, civil liberties and computer science to ask if they would provide a short essay on their views about privacy and DPI. The essays offer a variety of perspectives and divergent opinions.

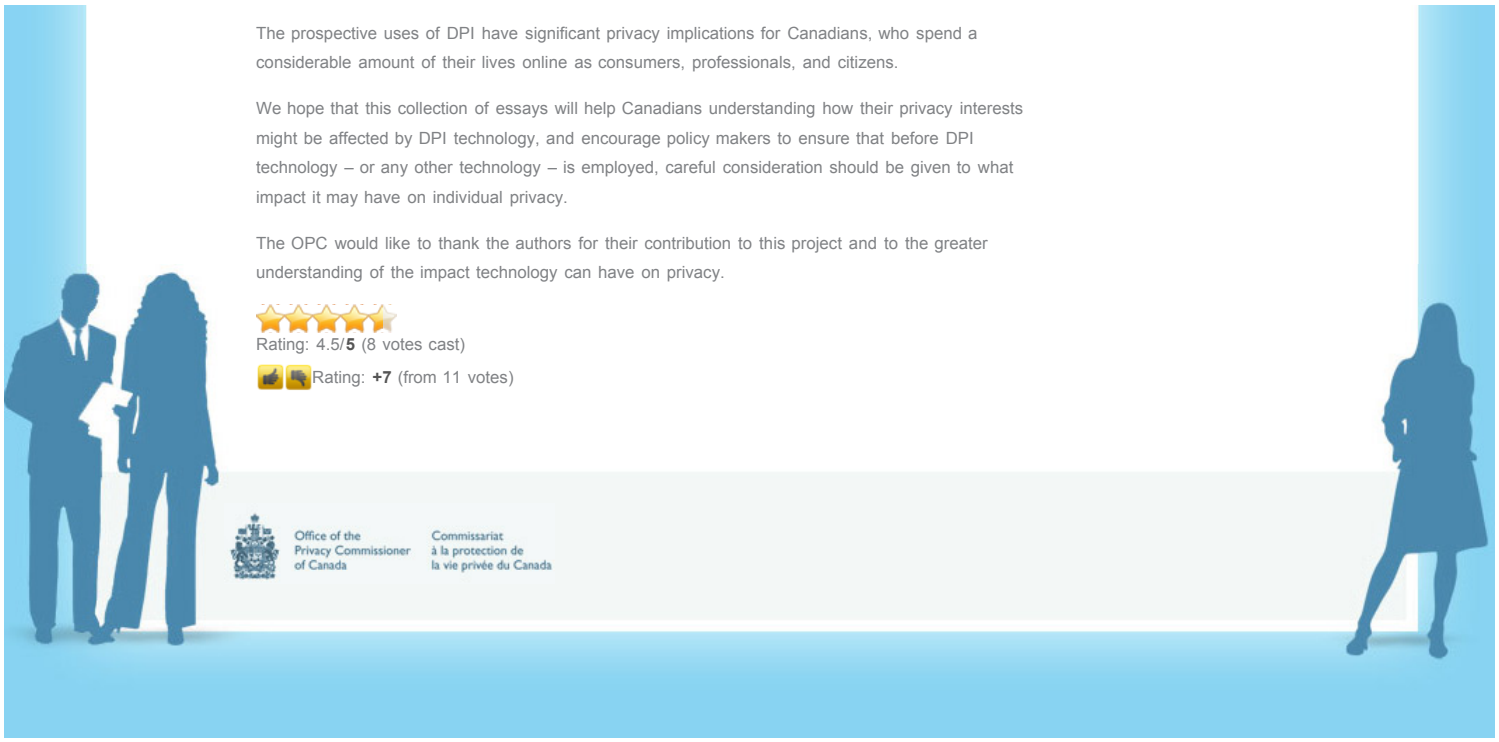
At nearly the same time, an opportunity arose for the OPC to contribute to a public discussion of the traffic management practices of Canadian internet service providers. The Canadian Radio-television and Telecommunications Commission (CRTC) called for written submissions to be received by February 2009. Public consultations are planned for July 2009.

The OPC welcomed the opportunity to contribute comments focused on the privacy implications of the potential uses of DPI. The submission was a logical extension of the OPC's legislative mandate to protect the privacy rights of individuals, foster public understanding of privacy, and promote the privacy protections available to Canadians. It is for this reason that we include it in this project.

Our submission made the case of privacy. We identified why privacy is important and how legal and public policy has historically recognized the rights of Canadians to the integrity of their physical person, their property, and their personal information – which includes their communications.

We did this to underscore two points. First, we wanted to show that privacy isn't a "new "or novel idea to which the state, industry and policymakers have only just recently turned their minds.

Second, our submission emphasizes that protection of personal information and privacy online is necessary in the face of market forces, rapid technological developments, the threat of ID theft, fraud, other criminal activity, and pressure from law enforcement investigations.



The prospective uses of DPI have significant privacy implications for Canadians, who spend a considerable amount of their lives online as consumers, professionals, and citizens.

We hope that this collection of essays will help Canadians understanding how their privacy interests might be affected by DPI technology, and encourage policy makers to ensure that before DPI technology – or any other technology – is employed, careful consideration should be given to what impact it may have on individual privacy.

The OPC would like to thank the authors for their contribution to this project and to the greater understanding of the impact technology can have on privacy.

Rating: 4.5/**5** (8 votes cast)

Rating: **+7** (from 11 votes)

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada