

Industry Canada

**Task Force on Spam:
Roundtable Meeting with
Key Stakeholders**

Ottawa, Ontario

December 3, 2004

Table of Contents

Opening Remarks and Overview	1
Chair's Remarks.....	1
Michael Binder, Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications (SITT) Industry Canada	1
Moderator's Remarks.....	2
Andrew Bjerring, President and CEO, CANARIE Inc.....	2
Keynote Address by Peter Coroneos	2
Public Education and Awareness: From Awareness to Action	4
Views from the Task Force.....	4
Suzanne Morin, Assistant General Counsel, Regulatory Law and Policy, Bell Canada.....	4
Bernard Courtois, President, Information Technology Association of Canada.....	4
Views from Stakeholders.....	5
Anne Taylor, Director of Marketing, Media Awareness Network	5
Bill Huzar, Secretary, Consumers Council of Canada.....	5
Michael Murphy, Senior Vice President, Policy, The Canadian Chamber of Commerce	6
Jannick Desforges, Counsel, Legal Services Option Consommateurs	6
General Discussion	7
Legislation and Enforcement: Does Canada Need New Legislation?	9
Honourable Donald H. Oliver, Q.C., Senator	10
Views from the Task Force.....	10
Roger Tassé, Partner, Gowling Lafleur Henderson LLP	10
Michael Geist, Canada Research Chair, Internet and e-Commerce Law, University of Ottawa.....	11
Views from Stakeholders.....	12
Heather Black, Assistant Privacy Commissioner of Canada.....	12
Ray Pierce, Deputy Commissioner of Competition, Competition Bureau, Industry Canada.....	13
Philippa Lawson, Executive Director, Canadian Internet Policy and Public Interest Clinic, University of Ottawa	13
Michael Eisen, Vice-President, Law and Corporate Affairs, Microsoft Canada.....	14
Paul Misener, Vice-President, Global Public Policy, Amazon.com.....	14
Gary Funderlich, Vice-President and General Counsel, AOL Canada Inc.....	15
Jay Thomson, Assistant Vice-President, Broadband Policy, Telus	15
General Discussion	16
Keynote Address by Joseph Alhadeff, Vice Chair of the Business and Industry Advisory Committee (BIAC) to the Organization for Economic Co-operation and Development (OECD), and Chair of the BIAC Task Force on Information Security	19
Discussion.....	21
Validating Commercial E-mail: Canada as a Leader for Certification.....	21
Views from the Task Force.....	22
Amanda Maltby, Senior Vice-President, Canadian Marketing Association.....	22
Neil Schwartzman, Canadian Coalition Against Unsolicited Commercial E-mail	

(CAUCE.ca).....	22
Views from the Stakeholders	23
John Levine, Co-chair, Anti-spam Research Group, Internet Research Task Force	23
Mitchell Wolfe, Senior Vice-President, General Counsel and Secretary, Visa Canada	23
.....	23
Sylvain Carle, President, Groupe Interstructure	24
Bernard Brun, Senior Counsel, Commercial et technologie Desjardins Sécurité	24
financière.....	24
Jay Aber, President, 24/7 Canada Inc.	25
General Discussion	25
Network and Technology Working Group: Beyond Best Practices	27
Views from the Task Force.....	27
Lori Assheton-Smith, Senior Vice-President and General Counsel, Canadian Cable	27
Telecommunications Association	27
Tom Copeland, President, Canadian Association of Internet Providers.....	27
Views from the Stakeholders	28
Gerry Miller, Executive Director, University of Manitoba	28
Alex Leslie, Vice President, Technology, AOL Canada Inc.	28
Mary Carman, Chief Information Officer, Industry Canada	29
Glenn Ward, Vice President, Customer Service Assurance, Bell Canada.....	29
General Discussion	30
Summary and the Way Forward	32

Opening Remarks and Overview

Chair's Remarks

Michael Binder, Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications (SITT) Industry Canada

Michael Binder, Chair of the Canada's Task Force on Spam, welcomed participants to the meeting and extended a greeting to those individuals listening via audio web cast.

"This meeting is an important milestone in the evolution of the Internet in Canada." Mr. Binder recalled working 14 or 15 years ago to promote the introduction of e-mail. Since that time, there has been an unbelievable increase in the use of that technology; however, there has also been an unbelievable proliferation of spam. In the last few years, spam has gone from being a minor nuisance to a significant economic and social issue. Today, spam impedes the effective use of e-mail by businesses and individuals and thwarts the growth of e-commerce. "It is time for all of us to work together to combat spam," Mr. Binder said.

In May 2004, the Minister of Industry announced the creation of the Task Force on Spam. The Task Force has taken a consultative approach to its work, bringing stakeholders together to work on this important issue. Five working groups were established to focus on specific issues related to spam. (Task Force members and members of the associated working groups represent more than 50 different organizations.):

- Legislation and Enforcement
- Technology and Network Management
- Validating Commercial E-mail
- Public Education and Awareness
- International Collaboration

The Task Force also reached out to Canadians using an online forum, as well as the *Canada Gazette*.

The objective of this roundtable meeting, Mr. Binder said, is for participants to take stock of the work that has been done to date, express their views and discuss future directions. He explained that he was also interested in hearing about initiatives that are under way in other organizations.

On behalf of the Minister of Industry, Mr. Binder thanked everyone for the work done to date, noting that the Minister is looking forward to reading the report that the Task Force will submit in the spring.

Moderator's Remarks

Andrew Bjerring, President and CEO, CANARIE Inc.

Andrew Bjerring said his role at the roundtable was that of “traffic cop”—moderating the discussion to help ensure that all important issues are addressed. Dr. Bjerring said that the agenda focused on four of the five working groups. International Collaboration would not be explicitly addressed, although this theme will run through discussions of the other four working group topics.

Keynote Address by Peter Coroneos

Chief Executive, Internet Industry Association of Australia

Bernard Courtois, President of Information Technology Association of Canada, introduced Peter Coroneos, explaining that two had met at the Organization for Economic Co-operation and Development (OECD) anti-spam meeting in Korea. “Although our countries are far apart geographically, we have much in common,” he said. Mr. Courtois noted that Mr. Coroneos’s organization deals with a broad range of issues related to information and communications technologies (ICT), including spam and cyber-crime.

Spam is a global problem that transcends activities in individual countries, Mr. Coroneos said. Australia has worked to deal with the issue through legislation as well as industry activities.

The Internet Industry Association of Australia was formed in 1995, and its members span every level of commercial economic activity. The Association also has global affiliations with industry associations in other countries, including Canada, with whom Australia has forged strong links. “There is a lot that we can learn from each other.”

The Association’s mission is to provide policy input to government about how to make the Internet a safer, faster, and more trustworthy tool—spam is a major issue. Mr. Coroneos added that Trojan technology now contributes to the spam problem. He recounted learning from an official at the World Bank that approximately 30% of computers have been infiltrated by Trojan technology. These computers can then be used to distribute spam undetected around the world. In fact, there are now turf wars being fought over these controlled machines.

“Phishing” is also a growing problem. This threat defrauds end users of their money, and institutions of the value of their brand. Identity theft is a byproduct of phishing.

Australia has taken a four-pronged approach to dealing with the problem of spam, addressing legislation, industry action, user empowerment, and international co-operation.

Legislation is effective because it can compel businesses to modify their practices. In

addition, spammers are often forced to move their operations, having an impact on the economics of spam.

The *Spam Act* was passed in 2003 and came into force on April 10, 2004, following a 120-day implementation period. The Act deals with all types of commercial electronic messages. Its intent is not to impede legitimate commercial activity by regulating messages that are purely informational, and it permits e-mail marketers to send unsolicited commercial e-mail as long as the mail contains the following:

- an opt-out mechanism (the company must respond to a request to unsubscribe within five business days)
- a functioning return e-mail address (active for 30 days)
- a valid subject line indicating it is an advertisement
- the legitimate physical address of the mailer

The Act also prohibits the use and supply of address-harvesting software.

As well, there is no bulk requirement in the Act; therefore, even a single e-mail message can be seen as spam. The focus is “not on the volume, but on the content of the message.”

Harsh penalties are associated with the Act, with violators subject to civil penalties of Australian \$1.1 million per day, along with injunctions. The decision was made to attach civil rather than criminal penalties to the Act because the standard of proof is lower in civil actions. A number of fines have been issued in recent months. Under the Act, regulators can extract an enforceable undertaking from companies (i.e., the company agrees to what it can and cannot do, and if it does not comply, it is taken directly to court). Since April, 70,000 reports have been made, 1,000 formal complaints launched, 800 inquiries made, and 150,000 hits reported on the website.

As part of the Act’s escalating penalties feature, 200 businesses have been warned to adjust their practices. Recognizing that most businesses are willing to comply with the Act, this escalation feature was put in place to give businesses that may have inadvertently contravened the Act a way to change their ways prior to the issuance of a formal penalty. This has resulted in a shift in the way businesses use e-mail to communicate.

Two industry codes of practice—one for Internet Service Providers (ISPs) and the other for e-marketers—have also been developed. With the Act, these codes are enforceable as law and help to further define the concepts that are included in the Act.

Since April, a number of spamming companies have moved their operations offshore, and Australia is now off the list of top 10 spam sources. In an attempt to educate users about spam and what they can do to combat it, Australian Internet providers have launched a trial to supply users with spam filters. An education campaign—“Don’t Try, Don’t Buy, Don’t Reply”—targeting consumer behaviour has also been launched.

Public Education and Awareness: From Awareness to Action

Views from the Task Force

Suzanne Morin, Assistant General Counsel, Regulatory Law and Policy, Bell Canada

Suzanne Morin acknowledged her working group co-chair, Geneviève Reed, Head of Research and Representation, Option Consommateurs, who was unable to attend the roundtable meeting. The Public Education and Awareness working group includes representatives from consumer and public interest groups, industry, and government agencies. The working group has two objectives:

- to identify and promote user practices and behaviours that can effectively control and limit spam; and
- to encourage and support the development of a multi-stakeholder public information and awareness campaign that would encourage end users in Canada to adopt anti-spam practices and behaviours.

Members agreed that individual users have roles and responsibilities in the fight against spam. The working group decided that the best way to make users aware of their role was to develop and disseminate clear, concise and realistic tips for users. These tips centre around three main themes: protect your computer, protect your e-mail address, and protect yourself.

Ms. Morin said she was pleased to announce that Friday, December 3, 2004, saw the launch of Phase 1 of the campaign, coinciding with the beginning of the online holiday shopping season. Since the host site (www.stopspamhere.ca) went live on the previous Friday, there have been 5,000 visits—1,200 of which occurred on the previous day. Dozens of other sites have agreed to display the campaign's icon and have a link to the main site, including Industry Canada, Consumer Connection, Strategis, the Competition Bureau, the Canadian Marketing Association, and Media Awareness Network. In addition, many private sector websites, including Telus and Magma, are displaying the icon, as are some university and provincial government sites.

Bernard Courtois, President, Information Technology Association of Canada

There were many different groups and interests involved in the development of Phase 1 of the campaign, making the process challenging but satisfying, Mr. Courtois said. Several companies (e.g., Rogers, Microsoft, Telus, and Bell) have helped to fund the campaign. Courtois suggested that a groundswell of support is occurring; e-mails are arriving from other companies that want to put the icon on their website.

Mr. Courtois asked the roundtable participants for their views on the campaign thus far, and for ideas about what should happen next. "What do we do to reach out to different people, like end users and small business?"

Views from Stakeholders

Anne Taylor, Director of Marketing, Media Awareness Network

Anne Taylor explained that the Media Awareness Network (MNet) is a national, not-for-profit, non-governmental organization that was formed in 1996. MNet's mission is to equip adults with the information and tools they need to help young people understand how the media work and affect lifestyle choices, and the extent to which they—consumers and citizens—are being well informed. MNet also provides reference materials for adults and youth to use to examine media issues. MNet also strives to establish media education as a cornerstone for consumers.

Young Canadians are global media consumers, Ms. Taylor said. Around the world there is growing recognition of what the media can offer, along with concerns about potential challenges and risks.

In 2000, MNet conducted a survey called *Young Canadians in a Wired World*. The survey showed that 53% of respondents had received spam sometimes or often; however, less than 20% of those respondents had told an adult about the spam. The survey also showed that 84% of youth are alone all or some of the time when they are online. In addition, many young people will give out their e-mail address in order to enter a contest. They are also not aware that answering a spam message serves to confirm their e-mail address.

Ms. Taylor added that 97% of Canadian schools are connected to the Internet and 86% use broadband.

It is important to equip children with the lifelong learning and critical thinking skills they need to manage the risks that they will face. Tips and resources to help young people make safe decisions are also required. Ultimately, these young people have to become sophisticated consumers, Ms. Taylor said.

Bill Huzar, Secretary, Consumers Council of Canada

The Consumers Council of Canada was incorporated in 1994 as a not-for-profit organization. The Council works to improve the marketplace for industry and consumers.

Mr. Huzar stated that the website and its tips are an important first step in raising consumer awareness, but only a first step—the problem of how best to publicize the website remains. The Task Force must reach beyond the Internet to engage all stakeholders. To this end, the Council has sent an invitation to its members, asking them to join the campaign. (Mr. Huzar added that he recently made a presentation to the Council's advisory committee, whose members are pleased that efforts are being made to address the problem of spam.)

The Council has asked its membership to help stop spam, recognizing that it is annoying

to consumers, can be costly to business, and can lead to loss of productivity. The resulting costs of spam are eventually borne by the consumer. The Council hopes to continue to work with its membership and the Task Force to help it meet its goals, Mr. Huzar said.

Michael Murphy, Senior Vice President, Policy, The Canadian Chamber of Commerce

Michael Murphy expressed his pleasure at being part of the Roundtable and having the opportunity to comment. He noted how important it is to recognize that the problem of spam goes beyond annoying e-mails. Spam has an impact on peoples' ability to use e-mail and can be used as a vehicle to distribute viruses and to facilitate identity theft. Consumers must be able to trust the marketplace; spam undermines that trust. Spam also clogs up the networks of small Internet service providers, meaning that time and resources are also tied up.

Mr. Murphy said that legislation is not necessarily an appropriate thing to focus on at the present time. Reviewing the current capabilities is a good first step. A variety of approaches—a tool kit—is necessary to combat spam. This tool kit should include a review of the current legislation, an examination of new technology, discussions with partners, and the development of information and support for consumers.

Information is needed to focus not just on consumers but also on the unique needs of the small business community. It is often difficult for small businesses to follow the tips that are disseminated for the general public as individual business practices vary, and may be more complicated to change. The challenge is to meet the needs of these small business users and to ensure that they are able to access reliable information they need to do business.

Jannick Desforges, Counsel, Legal Services Option Consommateurs

To solve the problem of spam, it will be necessary to undertake a series of actions, including providing information and education, said Jannick Desforges. However, it is not appropriate to reach everyone in exactly the same way with the same message, because not everyone is affected by spam in the same way.

Ms. Desforges said her group held a number of focus groups and undertook a number of surveys in the previous year. Findings showed that the 18- to 30-year age group receives more spam than the other age groups. This group is also more likely to use protective software and could benefit from information about how to protect e-mail addresses. Senior citizens, individuals with low incomes, and francophones are least likely to use anti-spam software. The message targeted to these groups should focus on the need to use anti-spam filters.

It is important for ISPs to provide better information to their users about how they can

protect themselves. This type of information could be provided upon sign-up and also with invoices. Anti-spam software could also be part of the start-up package, along with pamphlets that tell users how to protect themselves. Emphasis should be placed on the impact and danger of spam, focusing on the cost to consumers, the threat of viruses and identity theft, and the loss of server space. Consumers should be encouraged to be proactive and to rally against spam. There should also be a centralized point of contact to complain about spam. “Consumers [should] know that they have to share responsibility in the fight to control spam with industry, government and ISPs,” Ms. Desforges said.

General Discussion

Dr. Bjerring thanked the speakers for their contributions and posed the following questions to the participants:

- What actions or activities are needed?
- What is the role of ISPs in the dissemination of these messages?
- What tools should be provided?
- What are the most effective ways to reach different target groups?

A participant suggested that it might be interesting to structure the anti-spam campaign as a “white label” campaign. As such, each group could carry their brand as part of the promotion, and identify itself as a champion of the anti-spam cause. This might lead to better buy-in from industry and broader, more effective partnerships.

Mr. Coroneos said that it took him 10 days of e-mailing to build a coalition. In his e-mail, he outlined the problem, asked if the respondent agreed, and then asked if he/she would agree to carry the anti-spam message. The response was an overwhelming “yes.” Ensuring that the message was well thought out and grounded in reality helped to get this degree of buy-in, he said.

Mr. Courtois asked Ms. Taylor how she drew attention to MNet’s website and message. Ms. Taylor replied that her organization created a train-the-trainer model to get the message out. MNet has been successful in reaching most provinces and territories, she said, and has also recently launched “Reality Check,” a new resource that tells users how to be good Internet users. The group also has one person who is responsible for calling school boards and selling MNet’s interactive tool. As well, the group is a point of contact for many media, and its staff are often called upon to give interviews.

Responding to a question from Mr. Huzar about how best to build end-user empowerment, Mr. Coroneos said it is important to provide end users with the necessary technology and information. Australian service providers have been effective in this area. He added that he is impressed with Canada’s public awareness campaign.

Ms. Morin noted that the Canada anti-spam site has borrowed a number of slogans, including Australia’s “Don’t Try, Don’t Buy, Don’t Reply.” She added that in the last

five days the site has received hits from over 12 countries. The working group is considering adding to the information available on the website as part of their Phase 2 activities.

After commending the working group for their effort on developing the tips, a participant said that it is important not to forget that these tips will complement the education efforts that are already being undertaken by many ISPs in Canada.

Another participant asked if the working group has given any thought to how to provide consumers with the information they need in order to decide if e-mail is legitimate. He worried that this campaign might have a negative impact on legitimate marketers.

Mr. Coroneos replied that the Australian “Don’t Try, Don’t Buy, Don’t Reply” message is qualified with the following: “if you’re not sure who the e-mail is coming from or you have questions about its legitimacy.” This makes the message more complex than the simple tag line.

One participant told the group that it is necessary to emphasize the “protect yourself” tip. Consumers have to know that spam is not inevitable and that they have power.

Raising a question about the number of complaints that are received, one participant said that he has heard that people are not complaining—they are simply deleting the messages. Responding to a question about how Australia publicized the spam complaints process, Mr. Coroneos said that there was a lot of media interest when the act was introduced. “The government leveraged the outrage that was there,” he said. “People are complaining.” Another Roundtable participant said that he could assure his colleagues that there is a significant amount of consumer outrage in Canada. Canadians are now “trigger happy” and they are deleting legitimate mail. As a result, legitimate e-mailers are being hurt because of spammers.

Another participant raised the importance of communicating with members of Canada’s multicultural society. New immigrants are the fastest-growing group using the Internet, he said. It is important that any messages take new immigrants’ needs into consideration.

Maneesha Mithal, a representative of the United States, noted that the Federal Trade Commission (FTC) has an outstanding office of consumer education. Its website address is www.ftc.gov. The FTC has recognized the need to go beyond English-speaking messages and has introduced a Spanish-language initiative. It is important to leverage media interest in spam, and Ms. Mithal suggested the need to issue reports, give testimony, and enact new legislation.

Another participant said he would be interested in seeing Canada develop a “fridge” similar to that developed by the FTC. He suggested calling it Canada’s “freezer.” Canadians would then have a place to send their unsolicited e-mail. As it stands now, most Canadians do not know who to complain to. Echoing this sentiment, another participant said that even when people do complain, nothing is done about their

complaints. People stop complaining then, he said.

In Australia, the code of practice for Internet service providers includes the obligation to provide end users with information about how to make a complaint about spam. The young generation is very computer-literate and many youth think that spam is normal, a participant said. Any education program would have to take this generational difference into account.

Because the nature of the Internet is interactive, another participant suggested that the working group consider creating an interactive tool that would test a user's spam IQ. This type of tool could easily illustrate to the user what he/she is doing and the possible consequences of those actions. Tips only tell you something if you can situate the information, he added.

Spam is a broad social issue, one participant said. She suggested that Industry Canada could spearhead the formation of a centre of excellence that would bring people from industry, policy, advocacy and technology together with consumers to look at spam and its effects on society. Education is the first step, she said, but it is not enough.

Returning to the issue of Canada's multicultural population, a participant said that recent statistics show that visible ethnic minorities comprise 11.2% of the population in Canada's schools. She suggested partnering with the Canadian Teacher's Federation, the Canadian Library Federation, and SchoolNet to get information out to Canada's ethnic population about media literacy and media stereotypes. Another participant seconded the importance of working with schools and educating children. Ms. Taylor said that MNet is repeating its Young Canadians in a Wired World survey. She expects that this will generate a great deal of media interest.

Ms. Morin thanked the group for their feedback and suggestions, saying that the working group recognizes the need to get the message out better and to different parts of the population. Other issues that have been raised include the need to identify a contact point where users can make complaints. Users' expectations must be managed. She also mentioned that the group would look into the idea of a Canadian "freezer."

Dr. Bjerring invited participants, both in the room and listening via the web cast, to send additional comments to the Task Force.

Legislation and Enforcement: Does Canada Need New Legislation?

Dr. Bjerring explained that the first session had been a warm-up—a chance to feel good, converge on a set of issues, and get a good sense of how to proceed. He predicted that legislation and enforcement will prove to be a contentious issue.

Honourable Donald H. Oliver, Q.C., Senator

Senator Oliver expressed his delight at attending the meeting and the opportunity to overcome the problems posed by spam. He explained that he has been interested in preventing spam for some time, and has introduced two bills in Parliament to combat spam. The issue is crying out for a remedy, he declared.

When he began his study of spam, Senator Oliver realized that there is no single solution to the problem—partly because the Internet is fluid and borderless.

On September 23, 2003 Senator Oliver rose in Parliament for the second reading of an anti-spam bill (then called Bill C-23). At that time he stated that, “Canadian laws alone will not solve this problem,” and he went on to call for a multidisciplinary approach to end e-mail abuse. Many countries have introduced anti-spam legislation, he said. Currently, Canada has no laws, rules, or regulations specifically designed to cut down or track the source of unwanted communication messages.

Senator Oliver said that he might consider amending the bill depending on what he hears in the upcoming discussion. He told his fellow Senators that he would wait to hear from stakeholders before submitting the bill for second reading. Oliver is convinced that legislation has a role in the fight against spam, and he added that he would consider any suggestions that would strengthen his proposed bill.

Senator Oliver encouraged Industry Canada to initiate a national program that includes education, awareness and industry codes of practice. He said many Canadians feel happy that someone is taking action on this important issue. He also pointed to Australia as an example of how legislation can work. Australia has been successful in modifying the behaviour of spammers and getting them to leave the jurisdiction.

Views from the Task Force

Roger Tassé, Partner, Gowling Lafleur Henderson LLP

Roger Tassé offered his thanks to Senator Oliver for his persistence in attempting to draw attention to the issue of spam.

The first task put before the working group was to identify the obstacles that currently exist with the present legislation in the battle against spam. Mr. Tassé added that some laws do exist that, on first glance, seem to cover spam. Tassé stated that public lists of known spammers exist, and he wondered why these individuals are not brought before the courts.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA), which

was adopted four years ago, appears to guarantee the opt-out requirement and could be applied to the sale of lists across provincial or national borders. The Act could apply to spam, though the word “spam” does not appear in the Act. The *Competition Act* covers false and deceptive advertisements. Mr. Tassé questioned why this Act is not used more often against spammers. In addition, the *Criminal Code of Canada* could be used to charge spammers with fraud. “Fraud is fraud, whether it is off-line or online,” Mr. Tassé said.

Mr. Tassé asked the group why there was so little enforcement around the issue of spam. He posited that the lack of enforcement could be due to a variety of reasons, including a lack of resources, the complexity of the issue, the inadequacy of the existing legislation, and the fact that the issue is of low priority.

Mr. Tassé said that the working group still has much work to do before it reaches a conclusion on the issue. Working group members have met with the Office of the Privacy Commissioner and the Competition Bureau, and have also brought together groups of stakeholders and met with industry representatives to better identify the challenges facing the various parties involved.

All of these discussions have helped working group members have a better understanding of the issues surrounding spam, how destructive it can be, and how complex the issues are. “The jury is still out about the adequacy of Canada’s laws,” Mr. Tassé said.

While the working group might reach the conclusion that new legislation is necessary, Mr. Tassé reminded the group that legislation without enforcement and resources does not work.

Mr. Tassé said the Roundtable participants and the working group members have to decide exactly what that legislation would focus on, if new legislation were necessary. Would it be used to reduce consumer annoyance, protect consumers’ privacy or protect them against fraud? In order for the working group to be successful in persuading government to provide more resources in the fight against spam and to make it a higher governmental priority, the group will have to successfully illustrate the evil that spam poses.

**Michael Geist, Canada Research Chair, Internet and e-Commerce Law,
University of Ottawa**

Michael Geist explained that the Office of the Privacy Commissioner issued its first anti-spam decision a few days before this roundtable meeting—he was privy to this information because he was the complainant. He brought his complaint against the Ottawa Renegades, who persisted in sending him information even after he had asked to be taken off of their e-mail list. Dr. Geist complimented the Commissioner in taking such a strong position against spammers.

The decision in this case touched on a number of important issues:

- The complainant's business address is personally identifiable information.
- Although the defendants had obtained the complainant's e-mail address from the university's website (which is publicly available), the Commissioner ruled that their use of the address was secondary to its intended use and therefore outside of the existing exception.
- The complainant attempted to opt out, and the defendant did not abide by that request.

Although this is a strong decision, Dr. Geist said it does highlight the shortcomings of the existing legislation. In this case, the defendant has changed its business practices—which likely would not have happened if the complaint had been brought against a true spammer. The only other redress before a complainant is to take the defendant to Federal Court.

Other issues that are before the working group include the question of private right of action. Deceptive e-mail practices (e.g., false or misleading headers or subject lines) should also be examined. In addition, spam technology (e.g., harvesting tools) requires closer examination. Dr. Geist liked the idea of a Canadian “freezer” because it would help with the gathering of evidence.

Views from Stakeholders

Heather Black, Assistant Privacy Commissioner of Canada

Heather Black expressed her pleasure at being part of the Roundtable and speaking publicly about Dr. Geist's complaint to the Commissioner. She noted there were many debates in the office about whether a business e-mail address constitutes private information.

Ms. Black said PIPEDA could be used to combat spam because it has jurisdiction over organizations that are engaged in consumer activity (e.g., list brokers, data miners, and spammers). She explained that three provinces (Quebec, British Columbia and Alberta) have legislation similar to PIPEDA, and she will discuss the issue with these provinces.

Ms. Black admitted that there are limits on enforcement; her office can only deal with one case at a time. She said she hopes that rulings such as the one in the Geist case will be recognized in the community and followed by legitimate marketers.

“The name and shame route will not work with spammers,” she said, and she would welcome a complaint against a legitimate spammer. Her office has the authority to enter business premises, compel witnesses, and confiscate servers, she said.

Ray Pierce, Deputy Commissioner of Competition, Competition Bureau, Industry Canada

Ray Pierce reminded the group that the Competition Bureau is an investigative agency, not an enforcement agency. As such, the Bureau has no ability to order spammers to stop what they are doing. However, there is no reason why the *Competition Act* should not apply equally to spammers, despite the fact that there is no direct mention of spam in the Act.

Mr. Pierce told the group that the Bureau is investigating four spam cases. Three of these cases were brought to the Bureau's attention by the IT industry, and three (not necessarily the same three) deal with alleged misleading claims about health care products. In the spam messages—and it is the content of the messages that the Bureau is concerned with—the seller purports that the product can do something that is not likely the case.

More information is needed about the harmful effects of spam if the right legislative and enforcement measures are to be developed. People who commit these crimes are smart, sophisticated, and adaptable, and they use borders to avoid enforcement. “The criminals move at the speed of light, while enforcement moves at the speed of sound,” Mr. Pierce said. The challenge before the group is to design a framework that closes that gap.

Philippa, Executive Director, Canadian Internet Policy and Public Interest Clinic, University of Ottawa

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established over a year ago in the University of Ottawa Faculty of Law, Ms. Lawson told the group. CIPPIC's website (www.cippic.ca) includes a page on spam.

Ms. Lawson said the discussion about legislation flows nicely from the previous discussion about public education. “The way to communicate to people that spam is unacceptable is to pass a law that says so.” While legislation and enforcement are one piece of the anti-spam puzzle, there are many parts to the legislation and enforcement piece. There needs to be public enforcement of any anti-spam law that is enacted, she said. In addition, private parties that are affected by spam need to be able to go after the spammers.

There are private rights of action already in existence that could be used against spammers, but these types of actions are rarely used and are not tied directly to spam. In addition, the forum for action is often a barrier (the proceedings are time consuming and/or expensive) and the complainant has to prove damages, which is often difficult to do. There is also some opposition in Canada to private rights of action because they can be used to extort money from legitimate companies that may have only made an honest mistake. This fear could be dealt with by having the complainant prove a pattern of abuse.

She said the working group looked at the approaches taken in different jurisdictions (e.g., the United States, Europe, and Australia). The group's analysis of the various actions taken is included in the group's interim report.

Ultimately, any law enacted in Canada needs to be simple, needs to include the ability to follow the money, and needs to include remedies, including statutory damages.

Michael Eisen, Vice-President, Law and Corporate Affairs, Microsoft Canada

Microsoft supports a balanced, multi-faceted approach to combating spam, Mr. Eisen told the group. This approach should contain technological tools, industry campaigns, new legislation, industry self-regulation, and consumer education.

Globally, Microsoft has taken enforcement action against spammers by bringing forward civil spam cases and by identifying and referring spam cases to the appropriate governments. In total, Microsoft has brought 100 legal actions worldwide; 86 of those actions are in the United States. The actions have resulted in \$100 million in judgments.

Mr. Eisen said that success with enforcement is built on having specific anti-spam legislation. He believes that Canada should enact effective federal anti-spam legislation that should carry strong civil and criminal penalties and should include effective enforcement. The legislation should prohibit the use of false and misleading headers or subject lines, as well as the misuse of third-party computers. It should also prohibit the use of harvesting technology and dictionary attacks. In addition, incentives for the widespread adoption of best practices should accompany the legislation. With such a law in place, Canada could then be included in the global anti-spam actions that are being launched around the world.

Paul Misener, Vice-President, Global Public Policy, Amazon.com

Existing laws or new laws by themselves are not sufficient to eliminate spam. However, any laws that do exist or are newly enacted should be effective and not just symbolic. Mr. Misener provided the following guidelines for effective legislation:

- Most spam seeks money, so any legislation should follow the money to the ultimate beneficiaries of spam, the sellers.
- Legitimate commercial e-mailers will sometimes make mistakes. The legislation should only go after the companies who make a pattern or practice of spamming.
- Private plaintiffs, particularly ISPs, might have mixed motives, so anti-spam legislation should not trump anti-competition laws.
- Most legitimate companies accused of spamming will not want to go to trial. The legislation should make "pattern or practice" a necessary element of complaints and, thus, subject to pre-trial motions.

- Prosecutors have limited resources. Private parties should be allowed to gather evidence and help craft the prosecutions' cases.
- New anti-spam legislation should be uniformly applicable nationwide.

Mr. Misener explained that one principle factor in the passage of the U.S. federal act was the rise of conflicting state laws. He added that a national approach is preferable to many different state/provincial approaches.

Gary Funderlich, Vice-President and General Counsel, AOL Canada Inc.

Gary Funderlich said that he was glad to hear that the Task Force has established a working group to deal with consumer education. He has data that shows that a high percentage of users do not use the tools that are available to protect themselves. In terms of legislation, it is imperative that deterrence be paramount in any new laws that might be enacted. The business of spam is about money, so the penalties need to be sufficiently large to cripple the business aspects of spam.

Access is another issue. In the Canadian ISP community, only a handful of the 600 companies are large enough to sit at the table for these discussions. When the group talks about right of action, they have to remember that the majority of ISPs will not be able to fund or endure a long trial, nor will they be able to gather the necessary evidence.

In addition, the resource constraints on enforcement should be addressed. Whatever legislation exists or is enacted, regulators must have the ability to go after the spammers “with some teeth,” so that the resulting regulatory compliance activity is a deterrent to entering the spam business.

Jay Thomson, Assistant Vice-President, Broadband Policy, Telus

Jay Thomson said that he was pleased that Telus—a Canadian ISP based solely in Canada—was invited to be part of this roundtable. It is important to recognize that companies based solely in Canada might have different perspectives on the content and role of legislation and on the issue of private right of action.

Legislation is only one part of the solution to spam, Mr. Thomson said. Appropriate, narrowly targeted legislation can make a contribution; however, the group would be doing Canadians a disservice if that were all it chose to do. He stated that Telus supports a multi-faceted approach to combating spam.

The efforts of the working group have already had an impact; adoption of the group's recommended best practices has reduced spam complaints. Telus supports using the existing laws to combat spam, Mr. Thomson said. If these laws prove to be ineffective, then they should be amended. He said that enacting a stand-alone anti-spam law would do more harm than good. Such a law could target the wrong parties, inadvertently

sanction activities that should be outlawed, and raise the price that consumers have to pay.

Enforcement of the existing laws need to be in the hands of the bodies that are charged with protecting the public interest, and these bodies need the necessary resources to do their jobs, Mr. Thomson said.

General Discussion

Before opening the floor to general discussion, Dr. Bjerring asked Maneesha Mithal, Assistant Director for International Consumer Protection, U. S. Federal Trade Commission (FTC) to tell the group about the *London Action Plan on International Spam Enforcement Cooperation*. Ms. Mithal provided the group with background on what led up to the plan and said that the U.S.'s FTC had stepped up its efforts to combat fraudulent and deceptive spam, but was finding that much of the spam was originating outside the United States. While effective international networks have been established to deal with consumer protection, no such networks exist for spam, partly due to the fact that spam enforcement is handled differently in different countries.

On October 11, 2004, The FTC co-hosted the first meeting of spam enforcement agencies. There were 100 participants at the meeting. The outcome was the Action Plan, which has been endorsed by 19 agencies from 15 countries. The Action Plan is open to any public or private agency, which can then become a signatory to the Plan. The plan has three main points:

- Designate a point of contact for further enforcement communications under the Action Plan.
- Hold periodic conference calls.
- Take part in periodic special projects (e.g., respond to the OECD questionnaire on spam).

Mr. Tassé thanked the speakers for outlining the issues before the working group. There is a great deal of fragmentation in the distribution of responsibility to enforce the existing laws, a situation that does not help those individuals who wish to bring forward a complaint. Mr. Tassé said the concept of a Canadian “freezer” is interesting because it helps investigators identify and develop cases against culprits.

One participant said he wants to see a law that will deal with the criminals who send out spam messages. He said there were six spammers of significance in Canada today—a small number of people who generate a significant amount of spam, he said.

Senator Oliver asked Ms. Black if her office would be able to deal with a thousand complaints per month. Ms. Black replied that her office would not need to deal with that number of complaints; it would focus on genuine spammers, not legitimate e-mail

marketers that perhaps inadvertently contravene the law.

Mr. Pierce suggested that someone charged with a criminal offence is more likely to fight back. This could prove expensive and time-consuming, and outcomes are uncertain. In civil court, the spammer would be ordered to stop the activity, and the complainant could potentially get restitution. Civil charges would provide a more flexible way to deal with spammers, he said.

While private right of action seems good on paper, it is not realistic for most companies, said another participant. To make a dent in the problem, the law has to be able to put the worst offenders in jail for a long time, which has recently happened in Virginia.

Mr. Pierce cautioned participants about making comparisons to the United States, where criminal sanctions are very different. He said that jail time for a first offender in Canada is the exception not the rule. He added that it might be necessary to meet with the judiciary to make sure that they understand that spam is not a victimless crime.

Mr. Coroneos explained that Australia has decided to pursue civil penalties, which has proved to be an effective formula. In terms of private right of action, complaints can be laid on behalf of private citizens, and when those complaints are proved, any individual who has suffered a detriment can apply to the court for compensation.

Don Blumenthal from the FTC—the organization that manages the “fridge”—explained that the public mailbox (the fridge) is the primary method for consumer protection on spam. Mail to this address is sent to a large storage device where it is processed by a full text search program. This program allows prosecutors and lawyers to search the mail in the fridge.

Mr. Binder said that over the years he has heard some resistance from lawyers to changing existing laws. He asked if it is necessary to clarify the laws to reflect the new vocabulary that technology has brought to the table. “What is wrong with clarity in a focused bill?” It is important that this group have a voice in defining the problem and possible solutions.

Ms. Morin said “spam is nothing new; it is a new way to do existing bad things.” She said she does not think that new legislation is necessary; rather there is the need to define the issues and clarify existing legislation. In terms of private right of action, she said that today, if the Privacy Commissioner makes a ruling, individuals can go to Federal Court to seek compensation.

While in some respects spam is a new way to do things that have been done for a long time, some distinctions do exist, Dr. Geist said. Spam involves a cost shift that does not exist in other areas. In addition, because of spam, some people are turning away from e-mail as a valid form of communication. Legislation should be considered simply as one available tool to achieve policy objectives. Dr. Geist, in the discussion has heard some consensus emerging with respect to those objectives: the need for a deterrence effect,

likely through penalties or private right of action; the need for clarity in legislation and getting legislation “right”; and the need for additional resources to enforce the legislation.

Legislation that has criminal sanctions as well as large civil liabilities is also needed, so that enforcers are able to go after the people who damage consumers and the economy, a participant said. However, he noted that he has heard of a certain level of distrust from business regarding government legislation, and he has a feeling that business believes that government is trying to off-load its responsibilities in this area.

The Australian industry also felt some fear, Mr. Coroneos said. Some ISPs reported that if they tried to take a spammer off of the network, the spammer threatened legal action against the ISP. Under the new legislation, ISPs are immune from any action that a spammer might bring. The law governs what kinds of messages can be sent and under what conditions. The law has an impact on ISPs, he said, by codifying what good ISPs should be doing. Because industry has remained in control of the codes of practice, they have remained supportive of them. Mr. Coroneos said it is critical to have a clear law, strong enforcement powers, and well-resourced regulators.

Another participant said that the distrust that seems to be in evidence might be the result of the nature of the Internet business. Internet technology evolves daily, she said. Industry might be worried that legislation would freeze innovation in the sector. While it is valuable to identify best practices, industry might be worried that those best practices will become codified. That is not in anyone’s best interest, she said.

Ms. Lawson said the European Union directive that was passed about spam included the requirement that each member country adopt anti-spam legislation and include a private right of action. She asked if a private right of action is being considered to provide compensation to complainants or to be part of the deterrent to industry.

Ms. Morin said the issue before the group is that people do not know where to go to launch a complaint against a spammer.

Mr. Eisen suggested that the question does not seem to be whether there should be legislation, but what should be included in the legislation. The debate’s complexity should not deter the group from pursuing it. Mr. Eisen raised concern that the debate seems to be moving away from the need for a multi-faceted approach.

One participant noted that Canada is in the enviable position of being able to look at the legislation that was put in place in many different countries and take the best parts of the different approaches. He said that fining spammers is effective if the spammer is a corporate-like entity where the assets are evident. But this is rarely the case. The United States’ law removed a lot of the power that individual states had to go after spammers.

Mr. Misener explained that one principle factor in the passage of the U.S. federal act was the rise of conflicting state laws. He added that a national approach is preferable to many different state/provincial approaches.

Doug Lang of the Royal Canadian Mounted Police said that it would be difficult to raise the profile of spam with law enforcement officials. Today the national focus is on anti-terrorism and anti-gang activities, and resources are being put into these areas. The personnel, expertise, and will to go after spammers do not exist in the law enforcement community. He wondered if the Internet industry is thinking about how to pay for the necessary enforcement.

One participant suggested that the assets of spammers could be seized to help pay for the necessary enforcement. He warned that proxies and zombies could be used to turn off a city's 911 system. "We are sitting on the brink of disaster." Integration and intelligence about the spam problem is needed, another participant said, noting that spam content causes a continuum of harm.

Another participant called for better co-ordination between countries to address the problem of spam. Mr. Courtois agreed that the need exists for co-operation from countries where spam originates. He added that the number of countries taking action is greater than the number of those who are not.

Mr. Binder said that Canada cannot ignore the type of doomsday scenario put forward by one participant. It is time for action, he said.

Keynote Address by Joseph Alhadeff, Vice Chair of the Business and Industry Advisory Committee (BIAC) to the Organization for Economic Co-operation and Development (OECD), and Chair of the BIAC Task Force on Information Security

Bernard Courtois introduced keynote speaker Joseph Alhadeff, Vice Chair of the Business and Industry Advisory Committee (BIAC) to the Organization for Economic Co-operation and Development (OECD), and Chair of the BIAC Task Force on Information Security.

Mr. Alhadeff expressed his appreciation for the opportunity to address such an important subject. He reviewed the amusing attribution of the term "spam" to the comedy troupe *Monty Python's Flying Circus*, but said the term in fact pre-dated that use and began with early members of an online community of Dungeons and Dragons players. In response to a company's blanket e-mail advertisement, one player prompted the other members to send "coconuts and cans of spam" to the offending company. No doubt, Alhadeff said, the company that produces SPAM™ is not entirely pleased with the ongoing association of the meat product with undesired e-mail.

Mr. Alhadeff explained that thinking on this topic has evolved. Instead of creating definitions to define the problem—definitions that are outdated as soon as they are

complete—“now is the time to take action.” Spam, he said, is harder to kill than a vampire. There is no silver bullet for combating spam: legislation, technology, awareness, and enforcement individually don’t work. The solution must be a combination of all four. “Spammers read law. They don’t intend to follow it, but they read it.” Mr. Alhadeff said law has been in a vacuum, leaving it ineffective in countering spam.

Technology has great promise and can do great things, but “it is a means to an end” that must be used appropriately. It is not a solution in and of itself, nor is it a single industry. Many people are familiar with the actions ISPs are taking to counter spam, but the problem continues across industries, and groups and companies need to know what to do. Mr. Alhadeff supports as a helpful countermeasure the concept of not having open port relays.

Malicious spam ranges from “phishing” to “bot-herders” and “zombies.” Bot-herders sell connectivity on borrowed or stolen computer access, and harm is done as a result of all these things. “There is no question” that undesired commercial e-mail is a nuisance and contributes to network traffic. It is nowhere close to the problems caused by fraudulent e-mail that the sender “never intended to stand behind.” How can rules be enforced on these companies and individuals “whose identities will change tomorrow”?

Mr. Alhadeff explained that this is not the main problem affecting whether e-commerce will grow and flourish. If it were, “then inserts in magazines would be banned.” Focusing on the harm done by malicious spam, he posed the question of how best to address the problem, which, he said, has gotten worse with the involvement of organized crime. “Phishing raises by orders of magnitude the damage that was done” by earlier spam and the damage to the reputation of the companies whose identity is falsified on a spoofed website. Mr. Alhadeff recounted the creation of an entirely fictitious country online by a couple of men. This fictitious country had banking rules, laws, even an Olympic committee.

Spam is not just a nuisance; a keystroke reader, virus, or other malicious code might be imbedded in the e-mail.

Different companies can do different things to address this problem. Mr. Alhadeff recommended that companies “bring solutions to bear that are appropriate to your company,” involvement, and ability. “There is a dis-equilibrium of knowledge on this issue.” ISPs have done much to simplify the problem and make it more transparent, without taking control away from the consumer. Tools are being developed that will provide “indexes of reputation,” but while these will be helpful, they still won’t eliminate the problem of phishing.

“That,” Mr. Alhadeff said, “brings me to the role of government.” Is there enforcement to back up the discovery of someone phishing? If the activity originates in one country, but the cash flow is to another country, enforcement requires cross-jurisdictional rules. Mr. Alhadeff advises “thinking outside the can ... of spam” to find different ways to act. The FTC fridge is great, but now it holds millions of e-mail messages in a non-standardized

fashion, perhaps also non-searchable, nor useable for evidentiary purposes. “Perhaps we can make it more meaningful.” He suggested harnessing corporate filters and other corporate technologies that take spam off-line daily.

He noted, however, that the worst offenders are not the companies that send e-mail only to opt-in recipients; the worst are those sending e-mail that was never intended to comply with the law. No matter how good the filter, someone will always figure out a way around it. He attributed part of the problem to looking backward “when we look at the harm.” “We need to look forward” to get one step ahead of the creators of spam because they are constantly looking one step ahead to get around filters and other measures.

Companies will also need help from government to promote the importance of this issue and to educate the population about the costs associated with security and the products or services they may need to purchase, whether bundled, stand alone, or “cost plus.” Mr. Alhadeff suggests that some of the costs associated with fighting spam could be made back in savings that come from alleviating it “at the company gates.” He advised analyzing the economic externality to ensure “the right people benefit” and that spammers are stopped or at least penalized when caught. Canada could look into beefing up existing law, or packaging some other measures together.

Laws differ regionally and internationally, and while they may work in their respective countries, they also need to be able to “work together in a co-operative paradigm.” Mr. Alhadeff emphasized the need to keep moving forward to address spam issues as they come up, and to work better together. He supported stakeholder dialogue as the “best thing that can be done,” and said today “we are working for a consensus path forward.”

Discussion

The chair then opened the floor for questions. One participant asked how to stay ahead of the curve. Mr. Alhadeff used California as an example, saying the state had taken some good steps. But “California has also allowed bad facts to make bad law.” He advised taking a step back from the problems to see what is fact. Companies that have been targets of phishing attacks can provide information to help work toward enforcement solutions. “As filters get better, threats get more elaborate.” With phishing, a combination of consumer education about the validation of legitimate websites, as well as getting all stakeholders working together, may provide solutions and pre-emptive information. Banks, for example, that were targets of phishing, sent messages to their subscribers advising them that the bank would never solicit access numbers or other personal information by e-mail.

Validating Commercial E-mail: Canada as a Leader for

Certification

Views from the Task Force

Amanda Maltby, Senior Vice-President, Canadian Marketing Association

Ms. Amanda Maltby said this discussion was a good lead-in to the next issue on the agenda: validating commercial e-mail. The Task Force and the working group she is a member of have been looking at the issues surrounding spam from the perspective of legitimate communications. The mandate for the Task Force includes the examination of best practices for e-mail marketing, frameworks for Canadian marketers and businesses using e-mail marketing, and the possibility of an e-mail certification or authentication program.

“We’ve had a few face-to-face meetings” with ISPs, marketers and others to discover some of the problems surrounding deliverability. Some mentioned white and black lists, and as a result, the Task Force will be conducting a test to try to quantify some of these issues. Maltby said the group is also looking at codes, whether they exist globally, or, as with the CMA, in relation to a particular group or country, to determine what it can recommend as best practices. When deciding what should be put in place to improve the legitimacy of commercial e-mail, Ms. Maltby said it ultimately comes down to a question of cost and who should bear that cost. In considering e-mail deliverability, she said marketers want 100%, but ISPs may say that’s not a reasonable expectation. Therefore, an amount needs to be established that is reasonable. The Task Force is also looking into a certification program, and “we’d like more input on that today.”

Neil Schwartzman, Canadian Coalition Against Unsolicited Commercial E-mail (CAUCE.ca)

Neil Schwartzman then presented his views from the Task Force perspective. In screening for spam, he pointed out, false positives did not exist five years ago. But “as filters are ratcheted up” to keep servers online, the filtering mechanisms that process e-mail are sometimes producing false positive responses. This means valid e-mail from legitimate sellers and purchasers, or even the resulting credit card bill, is not getting through. Instead, it becomes collateral damage as filters become more diligent in order to fight spammers. “The spammers have created this problem.” Mr. Schwartzman said certification could become an issue for smaller operators. A large online business like eBay can provide verification and ensure its suppliers will carry the e-mail, but smaller operators and individuals may have more difficulty.

Calling a per-message cost “untenable, even the ¼ penny suggested by Bill Gates” would be an onerous collection task and ultimately profitable only for whatever organization collected all those quarter-pennies. He said alternatives like sender-bonding—in which senders put up an amount of money that may be collected as a fine if a specified number of complaints are made against them—may be more possible. But there also must be a measure defined by ISPs and users in the marketplace.

It has been suggested that Canada would be a good testing ground for such measures, and Mr. Schwartzman suggested that participants could read through the background documents provided for the roundtable discussion for more detailed information on these points.

Views from the Stakeholders

John Levine, Co-chair, Anti-spam Research Group, Internet Research Task Force

John Levine presented the view from the stakeholders' perspective. He said ISPs are buried in spam that forces them to use expensive filter services, yet mail senders have only paid for their own Internet connections, not those of their mail's recipients. The deliverability may be perfect through the outgoing ISPs carrier lines, but may encounter problems on the carrier used by the recipient's ISP. Mr. Levine said he doesn't mind receiving promotional notices by e-mail from Land's End (a retailer in the U.S.), but it wouldn't bother him not to receive it either. The business, however, would mind.

He also said Canada would be a good place to examine and test approaches to counter and filter spam because it has a smaller population than the U.S., has a lot of ISPs, and Canadian companies understand these issues better than many companies in the U.S. Although it is possible to have a single set of regulations for Canada and the U.S., Mr. Levine said the idea is not practical because there are too many differences between the countries. First among these differences is language—English and French in Canada, English and Spanish in the U.S. He also said that in the U.S., “we are way behind you” since this Task Force and group are already thinking about the issue. Mr. Levine would endorse a certification process that is specific to Canada.

Mitchell Wolfe, Senior Vice-President, General Counsel and Secretary, Visa Canada

Mitchell Wolfe offered the perspective of a corporation that participates in providing an electronic payments infrastructure. He recounted a recent study conducted by Global Insight and sponsored by Visa that showed electronic payments contributed significantly to the growth of the Canadian economy in recent years. He described electronic payments and the electronic economy (e-economy) as “built on a foundation of consumer trust and confidence.” Lately Canadians are concerned about protection of their information, and failure to protect it will undermine confidence in the e-economy. “If people get too afraid they'll stop participating in the e-economy, and if they stop participating in it, it will fail.”

Mr. Wolfe explained that phishing involves the use of fraudulent sites that appear legitimate in order to elicit personal information such as bank account numbers and credit

card information. A recent Visa-sponsored survey showed that only 16% of Canadians with Internet access or e-mail were familiar with the terms phishing or brand-spoofing, and even when the terms were explained, only 27% were familiar with these growing practices. Mr. Wolfe said most Canadians know not to fall prey to these scams, but 4% of those surveyed admitted being victims of phishing scams. This represents a minimum of 200,000 Canadians. Visa employs a company to monitor the Internet 24 hours a day, 7 days a week, to discover and shut down fraudulent Visa websites. Mr. Wolfe observed that significant investment is required to maintain Canadians' confidence in the integrity of e-payments and the e-economy and said his company supports the call for the close co-operation between government and business in addressing this issue.

Sylvain Carle, President, Groupe Interstructure

Sylvain Carle offered his perspective as a technology consultant representing SMEs. Saying that he could not live without his computer, Mr. Carle emphasized that e-mail should be accessible and remain usable. The technology practices under discussion are being put in place to identify and correct problems arising from the original e-mail design, which is open and decentralized. Having a centralized way to identify someone was not part of the original philosophy, and "I think we should keep that philosophy."

Any process adopted needs to allow small organizations to still be a part of the Internet. He agreed with the tone of the discussion that distinguished between legitimate commercial e-mail that is not harmful—although potentially annoying to some—and malicious spam. The e-mail messages from malicious spammers are the ones that get by the filters because "they have the time and money to work around" the restrictions. Mr. Carle said he hoped restrictions would not be a part of any legislation, but instead that there will be a common code of practice in the industry.

Bernard Brun, Senior Counsel, Commercial et technologie Desjardins Sécurité financière

Bernard Brun noted that there were not many financial institutions in attendance, and he thanked the Task Force for the opportunity to participate in the discussion. He said spam is by nature fraudulent and causes a loss of confidence and trust among consumers. The victims of spam are not only the recipients but also the businesses that lose access to this great opportunity. M. Brun said spam is beyond simply being an annoyance; it is becoming quite a contaminating factor. He explained his company's moratorium on all relationships with clientele by e-mail, and said that in terms of marketing, this is a major problem that needs to be solved. There are prejudices regarding e-mail that make it necessary to move in small steps. Companies need to remind people about unsubscribing, must gather client consent, and be able to prove that the client gave their consent. M. Brun said his company has been accused of spamming, and "there is nothing more dangerous for business" than to be labelled as a source of spam. The company had to trace each registration to discover when and where each person's name was added to their distribution list, and even the sentence used to provide consent. Data included a graphic

representation in the company archives to show this information.

While not every institution can provide this level of proof, these steps did alleviate the accusations of spamming. Speaking from his company's experience, he said it is clear that businesses need to reassure clients about the authenticity of the message they are receiving. His company is exploring authentication. Although certification is looked upon favourably, M. Brun said the cost is still an issue. Even were it to pay for itself, it is not a panacea.

Jay Aber, President, 24/7 Canada Inc.

Jay Aber said his company provides email marketing services to other companies. Figuring out whether a message is valid is a common difficulty, he said; the real challenge is determining if a message was delivered. In conversations with companies from eBay to major banks, this is the major issue. Even knowing for certain that a message was not delivered would be "something we could work with," but the uncertainty is a problem.

Mr. Aber expressed the view that government should not be involved in this issue. If the companies and people who deal with this issue on a daily basis "to make payroll" can't manage the problem, how could "anyone else get ahead of this?" He agreed with earlier comments that something more is required, but added that, with reports of limited resources from the RCMP to the ISPs, why not focus attention on the top "five or six really bad guys?" He said the process up to now has separated out the "really bad guys" from the legitimate business marketers.

General Discussion

With the floor open for questions, one participant said his company is working hard to try to stop spam, but it doesn't go away. He quoted estimates suggesting that 60–70% of e-mail traffic today consists of spam, and he questioned whether the number might reach 90% by next year. "We know what will happen to e-mail when that number reaches 100%." Millions of e-mail messages sent each day do not show up on spam radar because they use confirmed opt-in approaches and operate legitimately. He said filtering technologies can be based on keywords or the country of origin, but he cautioned that stacking these filters could create many instances of false positives and stop legitimate companies or organizations from reaching the rest of the world. "Phishing is huge" because there is a lot of money to be made. He echoed an earlier speaker's comments about the involvement of organized crime, saying it has latched on to ways of cleaning out bank accounts by phishing. This is an important issue because if phishing follows in the footsteps of spam, 80% of e-mail messages will be phishing in a few years because there is so much money being made from it now. If malicious spam finds legal ways to get through to opt-in users who want to allow only legitimate e-mail messages through, it

will affect their level of confidence and their use of e-mail.

Another participant said this problem has been addressed in web browsers by developing opt-in technologies and the use of the padlock icon on the browser that has become trusted by users. He asked why these options are not being applied to e-mail software as well. Another participant replied that phishing is more often used in search of identities, not just bank account numbers, regardless of whether it is on a legitimate SSL or a spoofed SSL.

Regarding phishing and identity issues in general, there is probably room for more than one level of identity verification. A retailer promoting a sale, for example, might need a lower level of verification than a message from a bank requesting the next mortgage payment. He suggested a centralized verification system that provides an industry specific branded signature. SSL certificates do require proof, but he said they are too easily obtained. "I could register any domain name and get an SSL certificate in 20 minutes."

Responding to an earlier speaker's comments that government should not get involved in this issue, Michael Binder said, "believe me, we don't want to get involved, but there is a limit to the length of time we will wait for a solution." Solutions have been talked about for two years and still haven't materialized. One participant compared the problem to curing cancer, but "does that mean it will never be solved?" If so, e-mail will never be the kind of economic driver that many hope it will be because users will lose confidence in it. The participant recalled a suggestion that Canada is a viable place to create a spam-free zone, and said, "maybe I'm dreaming in Technicolor" but "I think it's a legitimate question."

Another participant recounted his experience in Australia, where about 60% of the population uses online banking; a large percentage of those people have responded to a phishing e-mail message. Banks have approached their clients to provide authentication, but each is using its own system. So while there is recognition of authentication, there is still fragmentation. The government of Australia has stepped in to provide centralized methods to ensure people are who they say they are, and an organization is what it says it is.

Regarding padlock icons for e-mail software, the participant said there is no standard SSL system as there is in web browsers. He mentioned that AOL created a standard that all its e-mail will have a blue border; this method seems to work because the company has not uncovered any instances of AOL phishing.

Another participant suggested that it would be easy to solve the spam problem in Canada "if we were willing to cut off e-mail from the rest of the world." Using the previously mentioned comparison to curing cancer, he said it is easy to cure cancer if you don't mind killing the patient. "It's the freedom we're trying to preserve" that makes the issue a difficult one.

Mr. Schwartzman wrapped up the discussion saying he could set up an account, pretend to be eBay and send phishing e-mail telling subscribers they need to re-register their credit card. As with any bricks-and mortar-business, there are some who will shoplift and commit armed robbery. But if the public heard that armed robbery was up 50% last month and that government and law enforcement weren't doing anything about it, people would be in the streets demanding their money. If this weren't a virtual problem, "we'd need a bigger fan because so much stuff would be hitting it."

Network and Technology Working Group: Beyond Best Practices

Views from the Task Force

Lori Assheton-Smith, Senior Vice-President and General Counsel, Canadian Cable Telecommunications Association

Lori Assheton-Smith thanked everyone involved for their work in recent months to put together a working document so quickly, including input from industry members from the last 12 to 18 months, well before the Task Force was undertaken. ISPs undertook discussions on these issues with their competitors, knowing it is in their own and their customers' best interests to do so. "They did not do it because anyone told them to." She acknowledged that most of the recommended practices will make sense for some providers, but not all practices will make sense for all providers. She emphasized that the best practices are by no means a mandatory prescription for ISPs. Instead, she said, the working group tried to provide guidance for the community while leaving room for flexibility. These best practices are only one element of a multi-faceted approach to spam. Spam is about more than technology and so will the solution be.

Tom Copeland, President, Canadian Association of Internet Providers

Tom Copeland said there is a concept floating around that perhaps the industry isn't doing enough to prevent spam from reaching customers. It may be specific to each individual ISP, but providers are using many of the tools available. "We're identifying up to 80% of our traffic as spam," and that's what is getting caught in the spam traps. For his own ISP business, Mr. Copeland said the spam-filtering costs amount to the salary for one full-time position. As much as he'd prefer to keep that money here and employ someone, he needs to provide that service. Many ISPs in the market have already adopted many of these practices. The document will be reviewed to keep pace as technology evolves. Mr. Copeland said it is underlying principles that the group wants to promote, and he thanked "the folks in the trenches" who worked to solve some of these issues around how practices are adopted.

Views from the Stakeholders

Gerry Miller, Executive Director, University of Manitoba

Gerry Miller said universities and colleges are a kind of ISP and have similar restrictions and constraints. Spam was a huge problem, so his university adopted measures that include a bulk mail filter, a grey mail filter that requires sender verification, and a desktop virus filter. Mandatory use of virus software and mandatory patch management, both controlled centrally, were also implemented. In a university, Mr. Miller said, the words “mandatory” and “central control” were not popular concepts, but spam went nearly to zero and “I’ve had no grievances from the faculty union.” In this case, perhaps a legal framework is needed as backup, but that framework cannot hinder the technical solutions. Things like SPF and e-mail blocking have a different reception in an educational environment than in business. Spam costs a lot of energy and time, and in a public institution that is unable to pass the cost along to the consumer, it is a major problem. Time spent dealing with spam is time taken away from teaching and research.

Alex Leslie, Vice President, Technology, AOL Canada Inc.

Alex Leslie said his main message is “we cannot stop here.” It may have proved more difficult to get to some agreements than anticipated, but it got done. Whether agreement is needed among ISPs, or between ISPs and government, it is a necessary step. Speaking for AOL, he said the company is fully compliant already, and the processes implemented will have a greater impact if shared than if only implemented internally.

AOL has seen a steep year-over-year decline in spam delivered to AOL which we believe is on account of the success of our five-pronged anti-spam strategy. AOL Canada’s five-prong strategy focuses on Anti-spam tools provided to Subscribers, server-based filters and other host technology, litigation of Spam Kingpins, support for aggressive legislation against spammers, and industry collaboration and information sharing. We also provide a special AOL Postmaster site (<http://postmaster.aol.com>) for other ISPs to receive information about spam reports from AOL subscribers about that ISP, and bulk e-mailers to register for AOL's Whitelisting (and receive feedback about spam reports from AOL subscribers about them).

Mr. Leslie said AOL Canada is constantly on the lookout to try technologies that others have created as another tool in the arsenal of methods for effective filtering, including looking at third-party commercial certification organizations in the next year. Putting user tools in place is another approach to counter spam, and he said AOL Canada has seen a decline in spam reports from users over last year—an indication that the company is doing things right. Mr. Leslie recommended the formation of a society to “deal with issues among ourselves,” saying that providing mechanisms for people to communicate with each other quickly in order to alert others to problems and with an agreement to act quickly to counter it would be helpful. “We have not arrived, we’re on a trip” and need ways to work with each other and become more flexible than ever before. “As much as we’re glad to solve the problems of AOL, we’d be overjoyed to help solve the problem

for all of you.”

Mary Carman, Chief Information Officer, Industry Canada

Mary Carman said the role of an information officer in government may be different than at an ISP. Her tasks include maximizing the use of public funds, so affordability is a consideration at every step. She reviewed where the department hopes to be by 2008. Complaints from department staff indicate that work on spam filtering that has continued since 2003 has not been as effective as expected and the department had clearly reached the limits of the capability of the product in use. The filters blocked 6 million spam messages, but 21 million had not been filtered and were causing an increased demand on storage, server capacity and bandwidth. Spam was named as the number one harassment issue among departmental staff, and the annoyance factor is an element as well. “It was clear we needed to change now.”

Ms. Carman said the anti-spam approach was a leading issue raised in a computing workshop, and now the department has obtained the Secure Channel spam solution, provided through Public Works and Government Services Canada (PWGSC). The product has been modified to meet the specific needs of the department and “we intend to go forward with it.” There will be two tiers, and it will include a grey mail element. Once the anti-spam tool is in place, Industry Canada will also have an element to track outgoing mail that may not have been delivered. Rollout at Industry Canada is planned for January 8, 2005. Treasury Board is also preparing for a similar roll out, but Industry Canada grabbed the headlines and “we were in the paper” as spending \$5.5 million “because we had already quantified our business case.” Ms. Carman said this is an affordability solution for every department.

Glenn Ward, Vice President, Customer Service Assurance, Bell Canada

Glenn Ward, who is responsible for the sympatico.ca, bell.ca, and bellnet.ca systems, said Bell strongly supports the work done by the Task Force over recent months. These are not new procedures suddenly implemented, and “we strongly believe we need to be active within the ISP community” to face this challenge. “From today, I can see we’re making good progress.”

Profiling some of the specific things Bell has done to combat spam, Mr. Ward said the company was in a crisis situation in 2001, facing the prospect of being blacklisted by some American ISPs. The spam blocking that Bell implemented then has proven to be of great benefit over the last three years. In July of 2004, Bell implemented a 24/7 help desk as a single point of contact for ISPs to report problems in development, and for Bell to work with the ISPs through this and other more formal forums. Mr. Ward said this is often a bilateral discussion with ISPs to act quickly to shut down an attack.

At one time Bell noticed that “40% of our mail was being sent by 25 customers.” The company shut down service to those customers, and in many cases it turned out to be

unintentional spam from infected machines. During another outbreak, Bell quarantined dozens of customers in one day and contacted them proactively to address the situation. Mr. Ward said Bell has also seen a reduction in the number of complaints from customers, as well as a reduction in the amount of spam, and he credited both to the blocks Bell has put in place. He commented on other ISPs that are also being proactive and said that while spam is up and complaints are down, “it is not nearly over.” Mr. Ward said Bell is looking forward to working with Industry Canada and the Task Force in “continuing to fight the fight.”

General Discussion

The floor opened to questions, and one participant referred to earlier comments that the Australian and Canadian codes are similar. He said the difference is that the Australian code is instituted by ISPs but requires compliance bylaw, and he called the difference significant. Mr. Peter Coroneos said the code of practice in Australia has two parts. The main body is mandatory, but page 21 of the code sets out some best practice guidelines that are not intended to be mandatory. “We set out things many ISPs are already using” like blocking port 25 or limiting the rate at which subscribers can send out e-mail. The legislation doesn’t have any technological stipulations in it because as soon as you include technological rules it becomes outmoded and then there is no benefit to requiring industry compliance.

Mr. Coroneos said one mandated stipulation requires having a law enforcement authority contact reside in each organization. Spam filters or services are required and mandated, although he said most ISPs are providing these things anyway. A customer complaints mechanism is also mandated to ensure complaints are dealt with and “don’t just fall into a black hole.” He said when regulators say blocking port 25 sounds like a good idea and ask why it is not mandated, his association argues it is untenable for providers to require that. “We’re pushing back.” The code is due for registration before Christmas 2004 and will go through a consultation process. Mr. Coroneos said the code is there to foster best practices as they evolve.

Another participant asked if the Australian Communications Authority (ACA) has been an active regulator in requiring an mandate for the codes. Coroneos said this code would be the only one for spam, but there are other online regulations for children. Although the codes prompt headlines saying the Australian government censors the Internet, they are really regulations for ISP filtering. Further action is instituted only if the regulations are not implemented voluntarily. In order for such regulations to apply evenly across an industry, a regulator must go out and make it happen. He said Australia created a standard that would have called for fresh regulations if word got out that application was uneven and the process failed.

Another participant questioned the need for registration if it is indeed voluntary. Mr. Coroneos said it is a voluntary part within a mandatory code. “It’s a workaround.”

One participant restated his earlier comments on concern in industry about working toward voluntary codes in a quasi-regulatory environment—that something voluntary should suddenly become regulated. He said the many comments about money and effort in stopping spam and possible consequences to an ISP, including being blacklisted if they are not onside, will never lead to the resolution and co-operation Mr. Binder mentioned in his earlier presentation if the focus remains on legislation.

One other participant said blocking will not only reduce Canadian spam, it will drive peer pressure globally. He said, “I presented port 25 at Messaging Anti-Abuse Working Group (MAAWG),” and a telecom provider in Finland has completed implementation of port 25 blocking—and others are starting. Measuring the source of messages will also bring about a substantial drop and will guarantee mail delivered by users. He said his company receives only about 25 complaints per 1 million customers—a good reason to put spam procedures in place.

Michael Turner, ADM of the Information Technology Services Branch at PWGSC, said his division provides outbound services and connects directly into the main trunks of suppliers on the Internet. As an internal service provider, his division is also seeing the kind of concern around spam that Ms. Carman described. It is also implementing approaches for all departments, including PWGSC through the Secure Channel initiative, and looking into the possibility of putting the solution right on the server.

Regarding phishing, Mr. Turner said the Government On Line (GOL) program also falls under the responsibility of PWGSC, and staff in his department work closely with other departments and Treasury Board on this issue. He said the major challenge to getting clients and citizens online is the issue of public trust. PWGSC concluded some time ago that to guarantee this level of trust for sensitive transactions—financial or personal information—meant moving to a full Public Key Infrastructure-based (PKI) system throughout. Mr. Turner said this solution is far too expensive for commercial e-mail, and the government is only using it for sensitive e-mail. However, it is still one of the largest PKI environments in the world.

PWGSC will be following some of the best practices laid out today, but all the technical solutions for blocking spam aren't enough. Blocking will not be a full deterrent that requires a multi-pronged solution. “Let's not forget at the end of the day that we have a group of politicians backed by a group of angry citizens” that will be looking to public servants to implement a solution. Mr. Turner said when government staff are called upon to speak to the Minister on this issue, he wants to have the best solution possible in place for that. “Sooner or later we'll have to address that legislative agenda.”

Ms. Lawson said she heard a lot of people at table cautioning against technology solutions and saying it is inappropriate for government to mandate technology solutions, but she said she didn't hear anyone say that government should, or would, go that route. “I want to distinguish between the legislation that may be proposed” and what many are cautioning against.

Another participant said most of what he'd wanted to say had already been mentioned, but speaking as a lawyer, "the train is coming" and Canada needs to be on board with the best experience. He said he had received seven spam and two phishing e-mail messages on his Blackberry just during this meeting. In spite of the thousands of dollars his firm has spent to address the issue, "it is clear it is not enough."

Mr. Copeland said "we've heard some common threads today," some implied, some explicit in terms of fear. But when the Senate and House of Commons start working on this project, they won't have the same working knowledge that this group does, so they will be looking to industry for explanation and assistance. Their reality is what they see every day as users and customers.

Regarding earlier comments that no one is complaining about spam, it is a perception issue that needs to be addressed. "Even the big guys" can't dent this unless all levels are working together. Cost is an issue and neither government nor industry has the ability to recoup that cost. He said Internet service is one of the most competitive industries there is, and costs don't increase incrementally year to year. If businesses can enjoy some better utilization of networks, that's great but cost recovery is difficult to realize. For ISPs, Mr. Copeland said the key to the Australian law is that technology is not mandated. Activities are, but technology continues to be a business decision. "We are making progress with the Task Force," he said, and he thanked the co-ordinators for bringing the group together.

Another participant clarified an earlier remark that technology shouldn't be mandated, but it is all right to mandate the principles. The participant stated that the issue in question is mandating anything on industry, technology or otherwise. The chair thanked all the presenters, speakers and participants for their input throughout the day.

Summary and the Way Forward

Michael Binder said that rather than reading through notes and trying to put everything in context, he would share some of his observations from the day. He hoped the day had resulted in some ideas for moving forward tomorrow, and he offered congratulations on the icon the Task Force adopted to raise consumer awareness. It is a message, and as a consistent message, it may become well known.

The day's discussion ranged from children to SMEs and language differences. Mr. Binder said he was fascinated to learn that francophones are less likely to use a lot of security provisions, noting that that might be a point to follow up. Saying he kept hearing that no one is complaining about spam, he said personally he wouldn't know who to complain to, so that is not necessarily an indication that things are going well. He said the bottom line is that parliamentarians are anxious to act. Given a "minority government, you draw your own conclusions."

He noted the “good debate” on the right of private action, and helpful hints from the multinationals. Some good practices exist, so “let’s not reinvent the wheel.” Instead, he supports learning what works and what doesn’t in other jurisdictions. There was a great deal of discussion on deterrents, which bears further investigation. As well, the concern about raising consumer expectations needs to be dealt with.

Regarding following the money trail, Mr. Binder said that, while he liked that recommendation, it is easier said than done. How does one follow the money? It is not the ISP at fault, but the spammer. “Do we need a Canadian fridge or freezer?” If so, where should it be and who should operate it? Mr. Binder said he would be looking for some answers.

Mr. Binder said the Task Force would consider how to validate commercial e-mail over the next few months. More discussion will be needed around this point. “Perhaps brighter ideas will come from further dialogue.” He said that others have told him that it is a major accomplishment to get network managers, technology companies and the others in this group to all sit down together in Canada and propose solutions. “I see it a lot and don’t consider it a big deal, [but] maybe it is a big deal.” It is a *good* deal if it works and there is a lessening of spam. “I’m told it is working.”

Mr. Binder said Canada has a long tradition of voluntary codes. Many at this meeting had also worked on the privacy code, which was voluntary before it became mandatory.

Referring to benchmarks, Mr. Binder said that “Australia got it right,” and with respect, he would like to “do it better than you guys.” In closing, working together in partnership in Canada—government, industry and consumers—that is the right way, and there is still more work to be done. Mr. Binder invited further input through the Task Force website.