COLLABORATING TO ELIMINATE SPAM AND NUISANCE COMMUNICATIONS

IIC 2016 – COMMUNICATIONS POLICY & REGULATION WEEK

11 OCTOBER 2016, BANGKOK, THAILAND

Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

Canada

Cat. No.: BC92-94/2017E-PDF

ISSN: 978-0-660-08310-0

Unless otherwise specified, you may not reproduce materials in this publication, in whole or in part, for the purposes of commercial redistribution without prior written permission from the Canadian Radio-television and Telecommunications Commission's (CRTC) copyright administrator. To obtain permission to reproduce Government of Canada materials for commercial purposes, apply for Crown Copyright Clearance by contacting:

The Canadian Radio-television and Telecommunications Commission (CRTC)
Ottawa, Ontario
Canada
K1A ON2

Tel: 819-997-0313
Toll-free: 1-877-249-2782 (in Canada only)

https://applications.crtc.gc.ca/contact/eng/library

Photos: © ThinkStock.com, 2017

© Her Majesty the Queen in Right of Canada, represented by the Canadian Radio-television and Telecommunications Commission, 2017.
All rights reserved.

Aussi disponible en français

CONTENTS

ACKNOWLEDGEMENTS

The CRTC wishes to thank all contributors who participated in this workshop, without whom this report would not have been possible. In particular, the CRTC wishes to thank the following experts who contributed as speakers and moderators, generating a fulsome and interactive discussion.

- **Richard Bean**, Acting Chairman, Australian Communications and Media Authority, Australia
- **Chris Chapman**, President, International Institute of Communications
- **Stephen Eckersley**, Head of Enforcement, Information Commissioner's Office, UK
- **Adriana Labardini Inzunza**, Commissioner, Instituto Federal de Telecomunicaciones, Mexico
- **Travis LeBlanc**, Chief, Enforcement Bureau, Federal Communications Commission, USA
- **Tony Li**, Assistant Director (Support), Office of the Communications Authority, Hong Kong (Special Administrative Region)
- **Peter Merrigan**, Senior Investigator, Electronic Messaging Compliance Unit, Department of Internal Affairs, New Zealand
- **Christine Runnegar**, Director, Security and Privacy Policy, Internet Society
- **Dr. Steve Unger**, Chief Technology Officer and Group Director for Strategy, International, Technology and Economics & Board Member, Office of Communications, UK
- **Viola Veiderpass**, Digital Crime Officer, Cybercrime Directorate, INTERPOL Global Complex for Innovation

The CRTC would also like to thank the International Institute of Communications for its support and strategic partnership on this workshop. Special thanks to **Andrea Millwood-Hargrave**, Director General, and **Amanda Crabbe**, Director of Programmes, for their invaluable guidance, leadership, and contributions to this event.

As regulators, we must remain adaptable, open to collaboration, innovative, and resourceful. We do this by working together and by exchanging ideas in venues like this one...

Jean-Pierre Blais, Chairman and CEO, CRTC
Bangkok, Thailand

BACKGROUND

On 11 October 2016, the Canadian Radio-television and Telecommunications Commission (CRTC), in partnership with the International Institute of Communications (IIC), hosted a workshop on combatting spam and other forms of nuisance communications. The half-day event took place as part of the IIC's annual Communications Policy & Regulation Week in Bangkok, Thailand.

Like many communications regulators, the CRTC is committed to ensuring that its citizens have access to a world-class communications system – one that is safe, secure, and trusted. As part of this mandate, the CRTC is responsible for promoting and enforcing compliance with Canadian unsolicited communications policy frameworks. The CRTC also works continuously to improve its ability to collaborate with key partners – the private sector, domestic government partners, and foreign governments – in an effort to reduce harm to consumers arising from the abusive nature of unsolicited communications. The global nature of communications networks, and associated abuse of those networks, makes work across jurisdictions critical to success.

In partnering with the IIC, the CRTC sought the opportunity to further advance international cooperation on this important issue. The IIC provided the ideal forum for discussion, since it offered an independent, international, and distinguished platform to discuss the critical and evolving impacts of spam and nuisance communications on citizens and businesses globally. The IIC also offered access to a global network of senior-level industry strategists, regulatory authorities, enforcement agencies, academics, and other experts. The workshop introduced the IIC to the unsolicited communications enforcement community, and broadened the discussion of communications policy issues. Finally, the IIC provided an open and balanced environment for new ideas to emerge.

WORKSHOP OBJECTIVES

The purpose of this workshop was threefold. Its first objective was to bring together experts from both policy and enforcement communities around the world, enabling them to exchange views and experiences in policy, regulation, and enforcement related to spam and nuisance communications. These different communities are actively engaged in conversation and productive work to combat spam and other unsolicited communications. However, too often, these conversations take place in isolation, remaining mostly within each community; consequently, policy may be developed without sufficient consideration for enforcement needs, and feedback from investigators may not make its way back to policymakers, resulting in legislative barriers that hinder enforcement activities. Workshop participants were also requested to brainstorm on how to advance efforts to work collaboratively across borders. The discussions aimed to engage regulators from emerging economies and to introduce them to the work of established networks, communities, and organizations. As noted above, the global nature of these issues introduces unique challenges. While important considerations for anti-spam efforts can apply to both domestic and international initiatives, this report focuses primarily on international perspectives and approaches to working across jurisdictions.

Workshop attendees included 45 participants representing regulators from all global regions, industry representatives, academics, and other communications experts. The workshop began with a keynote introduction, which presented the main themes for discussion, described the impacts of unsolicited communications on governments and citizens, and outlined the current landscape faced by regulators and enforcement agencies. As part of the introductory keynote, workshop participants were also introduced to the Unsolicited Communications Enforcement Network (UCENet), an expert network of organizations engaged in international cooperation on spam enforcement.

The first panel, consisting of enforcement experts and practitioners, discussed three case studies detailing the international and cross-jurisdictional nature of the challenges in enforcing spam and unsolicited communications rules. The panel then discussed the challenges and opportunities in pursuing cross-border enforcement activities, including identifying the need for ongoing dialogue to ensure optimal enforcement and compliance strategies between countries. The second panel, consisting of policy and technical experts, identified capacity gaps and ways to increase harmonization of cross-border policies and enforcement activities. Discussions related to the opportunities and challenges specific to emerging economies. To conclude the workshop, an armchair discussion among senior regulatory officials identified the key takeaways from the first two panels and engaged all workshop participants in identifying next steps. A copy of the workshop agenda is available in **Appendix A**. All discussions during the workshop took place under the Chatham House Rule.

This report reflects a summary of the discussions that occurred during the workshop. The topics presented over the course of the afternoon frequently overlapped, highlighting the links between policy, technology, and enforcement challenges. The connections between issues and across areas of expertise were present throughout the workshop panel discussions. As such, the report reflects these themes, which are relevant to countries with robust anti-spam legislation and policies, as well as to those looking to rapidly grow their capacity and benefit from lessons learned.

REPORT HIGHLIGHTS

Based on the information shared by workshop participants, this report is divided into three sections. Part One identifies why, as an international community, there is a need to pursue cross-border collaboration on issues of spam and unsolicited communications. Unsolicited communications present a serious and increasing threat to the social and economic prosperity of the digital economy. Selling or stealing citizens' personal information, one of the major drivers behind spamming, has become a lucrative black market business. The public and private sectors share the responsibility to protect and educate citizens on this matter.

Part Two identifies interrelated challenges in pursuing enforcement activities. Unsolicited communications, whether initiated by legitimate or illegitimate actors, often cross borders, originating in one jurisdiction, but targeting citizens in another jurisdiction. This can raise legal challenges, while advancements in technology, such as the ability to spam anonymously, further complicate investigations. At the same time, different jurisdictions have different resources and expertise, which can either help or hinder capacity building for enforcement activities.

Part Three summarizes the consensus among workshop participants on the path forward. Specifically, participants agreed that interested communities (i.e. regulators; enforcement agencies; and interested third parties, such as industry or academia) should

- engage in ongoing and regular policy discussions;
- leverage private and public sector partnerships; and
- participate actively in UCENet.

No one organization can advance this agenda unilaterally. Policy makers and enforcement agencies must work together internationally, while also building robust domestic frameworks. The workshop represented an ambitious first step to start this work.

For an introduction to the fundamentals of spam and unsolicited communications, readers may refer to The Internet Society's Anti-Spam Toolkit and the report Best Practices to Address Online, Mobile, and Telephony Threats, prepared by the Messaging, Malware and Mobile Anti-Abuse Working Group.

01

WHY ACT NOW?

IT'S A SHARED RESPONSIBILITY

Combatting unsolicited communications – whether in the form of nuisance calls, spam, malware[1], or botnet infections[2] – is a priority for many governments that are committed to promoting growth and innovation in the digital economy. Online and mobile threats represent a significant risk to all economies wishing to benefit from the economic and social prosperity offered by the digital economy. In its most recent *Digital Economy Outlook*, the Organisation for Economic Co-operation and Development (OECD) explains that the digital economy:

> *... permeates countless aspects of the world economy, impacting sectors as varied as banking, retail, energy, transportation, education, publishing, media or health. Information and Communication Technologies are transforming the way social interactions and personal relationships are conducted, with fixed, mobile and broadcast networks converging, and devices and objects increasingly connected to form the Internet of Things.*[3]

Indeed, Internet and mobile technologies have revolutionized the way that commerce is conducted globally, as well as how governments operate and deliver services to their citizens. However, as more commerce and citizen engagement occurs online, new avenues are available for phishing[4], data theft, and other harm to consumers by malicious actors. Receiving an unwanted email, robocall[5] or Short Message Service (SMS) message causes, at the very least, consumer frustration and inconvenience. More detrimental outcomes can include fraud, breaches of privacy, and substantial financial losses.

Governments and the private sector alike have much at stake in combatting unsolicited communications: the damaging and deceptive effects of unsolicited communications can ultimately undermine citizens' trust in their communications networks, and more broadly, in the digital economy. The most nefarious spammers are shrewd and quick, and have a blatant disregard for the law. Eliciting personal information by deceit, or outright stealing it from unknowing citizens, has lucrative appeal in today's black market. In many cases, bad actors also thrive on their abilities to (i) hide their identities, (ii) abuse legal loopholes, and (iii) exploit multiple jurisdictions at once. In such an environment, they can set up and close shop quickly, making it extremely difficult for enforcement activities to be pursued.

In addition, the regulation and enforcement of unsolicited communications encompasses both civil and criminal law, engaging different enforcement bodies and triggering different legal frameworks. The technical nature of the issue also implicates network operators, as well as Internet and email service providers, while government departments and

[1] Malware is created or used by criminals to disrupt computer operations (see https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf).

[2] Botnets are groups of machines infected with malware that communicate (often through a complex network of infected computers) to coordinate their activities and collect the information that the individual malware infections yield (see https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf).

[3] OECD, Digital Economy Outlook 2015, OECD Publishing, Paris (see http://dx.doi.org/10.1787/9789264232440-en).

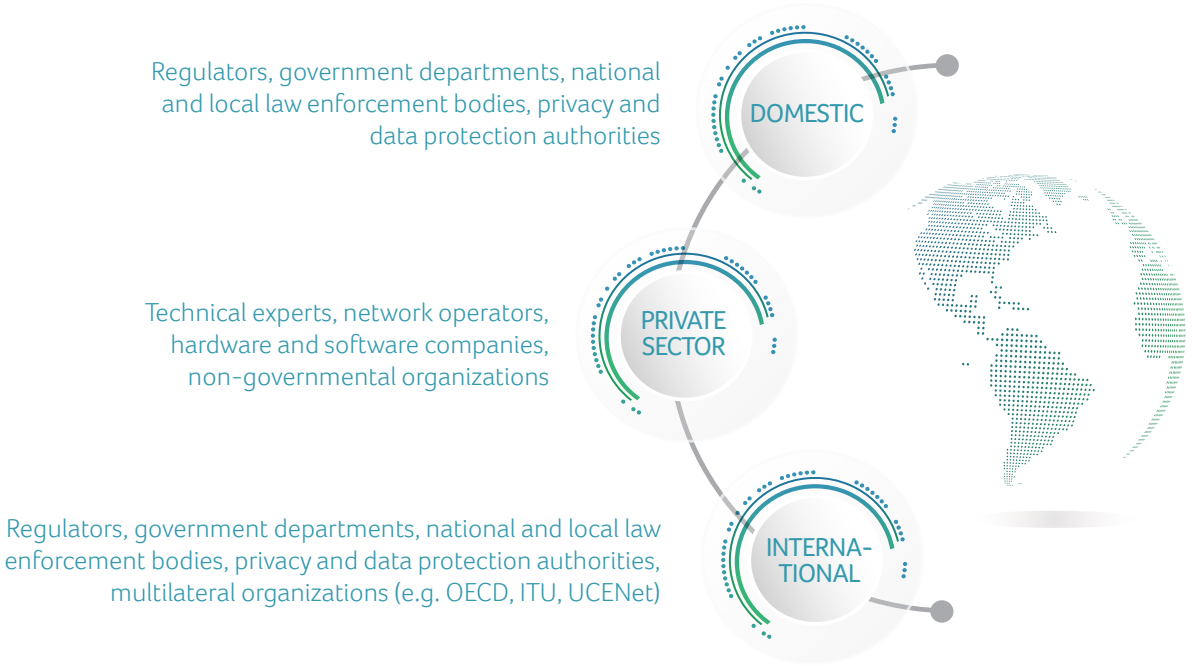
[4] Phishing refers to techniques that are used by malicious actors to trick a victim into revealing sensitive personal, corporate, or financial information (see https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf).

[5] Robocalls are unsolicited pre-recorded telemarketing calls to landline home telephones, and all autodialed or pre-recorded calls or text messages to wireless numbers, emergency numbers, and patient rooms at health care facilities (see https://www.fcc.gov/stop-unwanted-calls).

communications regulators often manage the policy and legislative aspects. The involvement of these different communities, each with their own objectives and mandates, further complicates the pursuit of a unified enforcement approach.

As highlighted throughout the workshop, combatting unsolicited communications is not a single problem, but rather a set of problems requiring a range of solutions. Anti-spam efforts are therefore a shared responsibility among several communities that must work in harmony: government and legislators, regulators, enforcement agencies, non-governmental organizations, the private sector, and technical experts. While the outlook on combatting unsolicited communications might appear bleak, there is good news. Many countries have made significant progress on this issue, particularly in enacting anti-spam and unsolicited communications legislation, promoting compliance with this legislation, and establishing domestic cooperation and international partnerships among different communities.

ANTI-SPAM COMMUNITIES AND PARTNERS



02

WHY IS IT A COMPLEX ISSUE?

THE CHALLENGES ARE GLOBAL, EVOLVING, AND REQUIRE THE COOPERATION OF MANY PARTNERS

Unsolicited communications are a global problem. Citizens in every jurisdiction are vulnerable to annoyance or attacks, regardless of the legal framework in their country. The challenges in combatting unsolicited communications derive in part from the multifaceted nature of the issue, touching areas such as policy, technology, and capacity building. The following sections aim to illustrate how these challenges are interrelated.

INCONSISTENCIES IN POLICY AND LEGISLATION

Developing legislation and policy to combat unsolicited communications is inherently complex. Unsolicited communications may come from either legitimate or illegitimate businesses, and violations can be civil or criminal in nature. For legitimate businesses, a clear civil framework combined with effective outreach can act as a strong incentive to understand and comply with the rules. With these tools in place, most legitimate businesses will comply, thereby protecting citizens from unwanted spam and nuisance communications. Although compliance frameworks often include remedies such as penalties or fines, workshop participants agreed that compliance is best achieved when regulators and enforcement agencies engage and support legitimate businesses through education, the sharing of best practices in compliance, and other outreach activities.

On the other hand, in the case of illegitimate businesses, there is a growing relationship between unsolicited communications and criminal activity. For example, an illegitimate business may use robocalls or spam to sell fraudulent products and services or to elicit personal information under the guise of legitimate business practices. Botnets may also be used to send spam messages containing malware or may be downloaded through links to infected websites. In these cases, the presence of a compliance framework and associated penalties does relatively little to limit abuse of the communications system. In addition, the deceptive or fraudulent nature of these activities may engage additional enforcement bodies (e.g. law enforcement bodies) and other legislative requirements (e.g. criminal frameworks), and often reaches across domestic jurisdictional lines.

In many cases, the act of sending spam messages falls under a civil enforcement regime. However, any fraudulent activity or inclusion of a virus in the message can be a criminal offence. In such instances, regulators and enforcement agencies must collaborate and share information with other law enforcement bodies that are mandated to pursue criminal cases. This can be challenging to do domestically, and more so, internationally. Engaging international partners that have different legal, policy, organizational, and cultural perspectives in the discussion can further complicate the process.

When enforcement agencies become aware of harmful activity, it is important to notify consumers of the activity to reduce the likelihood of fraud and to work collaboratively with any legitimate businesses that have unwillingly been comprised. For example, when a workshop participant's agency became aware of a robocall scam by offering travel and vacation deals using well-known household brands, the agency worked with the legitimate businesses to issue simultaneous advisories on their respective websites, alerting citizens to this activity and preventing further harm.

Regardless of whether the source of the unsolicited communications is legitimate or illegitimate, technology has accelerated the volume, speed, and most importantly, the ease with which violations may cross borders. It is not surprising then that the most malicious types of unsolicited communications often do not originate in the same jurisdiction as their target audiences. This, in turn, may cause legislative roadblocks, since it can be difficult to pursue cross-border cases without legislative authority or, at the very least, mechanisms for information sharing, such as memoranda of understanding.

These roadblocks derive from the fact that legislation varies widely among different countries. Inconsistencies or gaps in legislative frameworks in different jurisdictions can cause challenges in sharing information, pursuing effective enforcement, and seeking remedial action. For example, several countries host spam intelligence databases, which collect a high volume of emails infected with malware that have been sent from another country. Sharing this data between jurisdictions would further anti-spam efforts and enable more effective enforcement action. However, this data often contains personal information, and domestic privacy requirements can limit the ability to share this information (e.g. additional agreements and legal authority may be required). In addition, practical experience shows that enforcement powers can be difficult to exercise across borders. As one workshop participant pointed out, when dealing with a target of an investigation who is based abroad, issuing a fine without the legal authority to enforce it is an ineffective deterrent. However, progress is possible when jurisdictions work together to establish trusted partnerships.

Case study: Information sharing

One participant spoke of challenges in acquiring confidential information from a company outside its jurisdiction that was required to pursue an investigation. The company claimed that because its operations were located outside the participant's jurisdiction, it was not obliged to disclose its data, even though it was enabling illegal activity in the participant's jurisdiction. Fortunately, the participant's jurisdiction had a long-established relationship with the enforcement agency where the company was located. Together, they were able to use their respective laws to produce and share information lawfully to pursue enforcement action.

TECHNOLOGY ENABLES ANONYMITY

As technology continues to evolve, so does the sophistication of unsolicited communications. Advancements in technology have lowered costs, removed cross-border barriers, and given spammers easy access to a variety of tools that deceive and cause harm to consumers. Spammers are not only able to reach a wide audience with incredible speed, they are also able to easily hide their identities. For example, as one workshop participant explained, spam can be sent anonymously and from virtually anywhere in the world through over-the-top (OTT) applications (e.g. Whatsapp).

In fact, some OTT applications are designed with features that inherently facilitate spamming. For example, a chat application may not request additional consent from users before adding them to group chats that could potentially generate spam. Although such facilitation is often unintentional, its negative repercussions can result in various types of damages to consumers, such as personal identity theft.

Remaining anonymous is easy, even for an unsophisticated spammer. As one workshop participant explained, a spammer may use a prepaid SIM [subscriber identity module] card, which in turn provides them with a phone number (i.e. the only requirement to register for some OTT messaging apps). In many countries, the purchase of a SIM card does not require a subscription or registration; thus, tracking the spammer is likely impossible.

As another participant described, advancements in technology have affected unsolicited communications not only on newer platforms, but also on legacy platforms, including telephony.

For example, millions of citizens are affected by robocalls daily. One workshop participant noted that at least 21% of all calls made in their jurisdiction are robocalls (i.e. 1 in 5 calls). Technological factors have resulted in reduced costs of equipment and services, thereby contributing to the wide-scale volume of these calls. While robocalling used to require specialized equipment, today, the only equipment needed is software on a computer or mobile phone.

Robocalls have also become an international problem. As with the use of messaging apps or email for spam, the majority of robocalls are made based on the fact that callers are able to hide their identities. As explained by one participant, phone numbers are no longer associated with a unique physical address. Advancements in technology have made it easier to acquire multiple telephone numbers and to spoof[6] numbers.

Case study: OTT spam

OTT applications may enable spammers to add users to chat groups without obtaining any form of consent. A spammer may then form a chat group from a block of sequential phone numbers and send spam messages under the falsehood of promoting a particular business. The business being promoted may actually be a legitimate business that neither sent the message nor authorized its sending. In such an instance, the legitimate business may not be legally at fault, but finding the real source of the spam remains problematic.

[6] Caller ID spoofing occurs when illegitimate telemarketers change the information that appears on the caller ID display to misrepresent themselves and to trick the recipient into answering the call (see http://www.crtc.gc.ca/eng/phone/telemarketing/identit.htm).

Moreover, with the uptake of voice over Internet Protocol (VoIP) technology, high-cost international calls are no longer a barrier to casting a wide net of targets, meaning that it can be advantageous for robocalls to originate in foreign countries. While advancements in technology have made it much easier to send and receive unsolicited communications, they have also enabled spammers to take advantage of consumers, especially to fraudulently obtain funds.

From an enforcement perspective, if a spammer is untraceable, the next step is to follow the money. For example, when personal information is stolen for the purpose of reselling it (e.g. to apply for credit cards or loans) tracing each monetary transaction can lead to the scammer.

Technology has also enabled easy and direct payments between unknowing victims and spammers. In the past, the process of moving currency internationally was burdensome, and involved at least one third-party authority (e.g. a bank teller). Such a transaction would likely have been questioned at some stage by that authority. Today, money can be moved from one party to another with great ease – whether through gift cards, virtual currencies, e-transfers between bank accounts, or other online payment systems. With fewer opportunities to intercept transactions, spammers can collect fraudulent funds and vanish before a victim realizes that they have been deceived.

CAPACITY BUILDING FOR EMERGING ECONOMIES

While all economies face challenges regarding unsolicited communications, there are some notable differences in the challenges faced by emerging economies. As noted in previous sections, unsolicited communications have evolved to encompass much more than the occasional unwanted email. The threat landscape is considerably different today than when the Internet was first introduced to the public. In addition, in many developed economies telecommunications infrastructure – and associated misuse –has evolved over nearly half a century, while emerging economies have leapfrogged wireline technologies and gone straight to mobile communications technologies. Accordingly, as one workshop participant explained, emerging economies may face sophisticated spammers without having had the advantage of building their skills and resources when the threat was simpler.

The workshop participant further explained that there is often an abrupt and exponential growth in local Internet service users as broadband services become affordable within an economy. Many emerging economies are rapidly becoming predominantly mobile commerce economies. This may strain the resources of governments and new network operators alike that may be unfamiliar with the anti-spam communities and resources available to them. Without anti-spam legislation, frameworks, or participation in cooperative networks, emerging economies are more vulnerable to being attacked by spammers and to breeding them.

Another workshop participant discussed some of the challenges in partnering with countries having varied enforcement experience. For example, in one jurisdiction, an automated call may be considered a straightforward violation of anti-spam legislation. In another jurisdiction, this same call could be viewed as annoying, but still a harmless and legitimate business practice. If one party does not view the action under investigation as inappropriate, establishing trust and a willingness to cooperate may be more challenging.

03

WHAT'S NEXT?

GLOBAL PROBLEMS REQUIRE GLOBAL SOLUTIONS

Unsolicited and nuisance communications have no regard for borders, yet policy and enforcement communities face roadblocks such as inconsistencies in legislation, technology that enables anonymity, and the specific needs of economies with varied levels of policy and enforcement experience. The consensus among workshop participants was that to overcome these challenges, anti-spam laws and policies alone are not enough; neither is a unique focus on enforcement or technological solutions. In fact, as one participant stated, a collection of efforts and incremental solutions are likely more effective than a single grand design. Accordingly, workshop participants discussed possible activities to advance this work. Participants agreed that next steps require the active participation and cooperation of all stakeholders, including regulators; enforcement agencies; the private sector; and interested third parties, such as academia and non-profit organizations. These next steps are outlined below.

1. ENGAGE IN ONGOING AND REGULAR POLICY DISCUSSIONS

Regulators and enforcement agencies must carefully build agile regulations, polices, and practices that are efficient and effective or they risk hindering the competitive advantages offered by the digital economy. As one participant described, an effective regulatory approach requires balancing the need to create a hostile environment for businesses that deliberately target vulnerable members of society and creating an engaging and supportive environment for businesses that are doing their best to comply with legislation.

Another participant noted that concerted international collaboration is essential to target spam and nuisance communications not only when it occurs, but before it even starts. More often than not, international cooperation in the area of policy requires time, legal expertise, and formal written agreements, whereas the threats posed by unsolicited communications are often imminent and time sensitive. International cooperation is also difficult to accomplish without first establishing domestic policy and legal frameworks, and cross-sector coordination.

Workshop participants agreed that inconsistencies across jurisdictions (e.g. differences in legislation and lack of regulatory frameworks) can limit the ability to acquire and share the information required to pursue certain investigations. As such, workshop participants agreed that international jurisdictions with all levels of experience should engage in regular policy discussions to share expertise and best practices for enacting or reviewing legislation. These discussions would also serve to nurture relationships that would allow for improved information sharing and collaboration.

As noted by one participant, experience shows us that a quickly evolving system such as the Internet benefits most from an open, consensus-based, participatory approach to policy. This approach would involve multiple stakeholders and take into consideration the wide range of interests of people who have overlapping rights and responsibilities across sectors and borders. Accordingly, workshop participants agreed that an international forum – one that is either new or established – would allow for continued discussions on specific policy issues, such as the following:

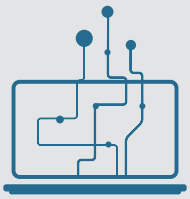
- What are "lessons learned" in drafting anti-spam policies and legislation? What is the best way to ensure that provisions are nimble for quick cross-border information sharing?
- How do we ensure that policy and legislative provisions are flexible enough to evolve over time, adapt to technology, and be responsive to new platforms and protocols?
- How can agreements between and among jurisdictions be improved or be more efficient?
- What is the role of citizens? What is the appropriate balance between security and privacy by design, and outreach and education to empower and inform citizens?

2. LEVERAGE PUBLIC AND PRIVATE SECTOR PARTNERSHIPS

Workshop participants agreed that legal frameworks and enforcement networks, both domestic and international, require input and support from private sector stakeholders. Specifically, the private sector can contribute technologies and commercial incentives as complements to traditional enforcement tools. Global network operators, telecommunications companies, and Internet service providers (ISPs), by virtue of their role in building and operating communications infrastructure, have a major influence in controlling the sending and receipt of spam.

Throughout the workshop, participants highlighted innovative anti-spam efforts that require private sector partnerships, such as the following:

SPAM AND NUISANCE COMMUNICATIONS INITIATIVES

	MECHANISM	EXAMPLE	DESCRIPTION
	Spam Intelligence Database (SID)	Intelligence Hub (ICO)	A tool for citizens to report spam and other electronic threats to government agencies. SIDs can also receive data from industry, providing additional intelligence to support enforcement actions.
	Short Code Reporting	#7726 or #Spam	When an individual receives an unsolicited message, they can dial short code 7726 or "spam," and the complaint is automatically forwarded to a database used by enforcement agencies.

	Industry Coalition Initiatives with Government Support	Robocall Strikeforce (FCC)	Technology and communication companies join forces to share information, work with regulators and consumers, and combat abusive communications more effectively.
	Research and reports	National Cyber Reviews (INTERPOL) Operation Safety Net (M3AAWG)	Enforcement agencies, private sector partners, and other groups are learning and sharing information on this rapidly evolving issue. These reports include reviews of legal and technical frameworks, identification of cyber capability gaps, and best practices for governments, regulators, and the private sector.

Accordingly, workshop participants agreed that engagement and partnerships with private sector stakeholders are critical in the development of multidimensional enforcement protocols. When illegal activity is discovered on telecommunications service providers' or ISPs' networks, sharing information is mutually beneficial for all stakeholders.

Case study: Threat identification

One workshop participant described a successful notification protocol through which an enforcement agency monitored the existence of malware and other electronic threats, and used that information to alert interested parties. These parties were then able to block or otherwise remediate the threats. Although enforcement activities could have been pursued after the event, this approach stopped the illegitimate activity as it was occurring, thereby reducing harm to consumers.

While law enforcement bodies are working diligently in many countries to be proactive in deterring threats domestically and across borders, a large portion of enforcement activities happen on a reactive basis, after the harm has already taken place. On the other hand, the private sector can provide valuable insight on threats in real time, by virtue of their position as network operators and technology experts. For example, if an ISP is alerted to an infection on its network, it can act immediately to shut down the malicious traffic that is overloading the system.

A major driver for success is to have processes and protocols standardized and shared with stakeholders both domestically and internationally. For example, ongoing dialogue between the public and private sectors is necessary to create two-way notification protocols that can be rapidly rolled out in the event of a breach. In addition, through the private sector's Internet security expertise, harmful activities (e.g. known command and control server[7] activity operating on a private partner server) can be detected quickly and effectively. This information can then be shared with law enforcement bodies, which can use their legislative tools, including search and injunction powers, to disrupt the activity and collect the information required to pursue enforcement action.

Private sector stakeholders all over the world are already working collaboratively on these issues. For instance, the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is an industry-led, confidential, and global forum dedicated to operational issues regarding Internet abuse. This group actively publishes best practice papers, position statements, training and educational videos, and other materials. It also provides technical and operational guidance to governments and public policy agencies regarding new Internet policies and legislation.[8]

Other important collaborators include different forms of Computer Security Incident Response Teams (CSIRTs) and non-profit organizations such as Spamhaus. CSIRTs are responsible for coordinating and supporting a response to a computer security event or incident within an entity (e.g. government, commercial organization, or non-profit organization); their goal is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.[9] The Spamhaus Project is an international non-profit organization that tracks spam and related cyber threats and provides real time intelligence to the Internet's major networks, corporations, and security vendors. Spamhaus also works with law enforcement agencies to identify and pursue spam and malware sources worldwide.[10]

3. PARTICIPATE ACTIVELY IN UCENet

Another vital resource that exists to promote cross-border enforcement cooperation is the Unsolicited Communications Enforcement Network (UCENet), formerly known as the London Action Plan. The objective of this long-established network is to promote international spam and telephony enforcement cooperation, and to address problems related to nuisance communications, such as online or telephony fraud and deception, phishing, and the dissemination of viruses.

Workshop participants agreed that participation in UCENet is critical to cross-border partnering in the areas of enforcement, intelligence, communication, and training. This community of enforcement agencies has long recognized that online and telemarketing activity is not bound by geographical or jurisdictional borders. Since many government agencies operate with limited resources, UCENet enables collaboration across skillsets and expertise, which reduces the duplication of efforts to achieve common goals. Its membership includes agencies from 27 different countries, government

[7] These servers are used to remotely send often malicious commands to a botnet or a compromised network of computers (see http://www.trendmicro.com/vinfo/us/security/definition/command-and-control-(c-c)-server).

[8] See https://www.m3aawg.org/

[9] See https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

[10] See https://www.spamhaus.org/organization/

departments, and other interested parties in private sector, non-profit organizations, and academia. The network provides opportunities to learn from each other's experiences from an enforcement perspective. Workshop participants recommended that additional governments and interested agencies become UCENet members to expand the reach and benefits of this network.

Participants in UCENet also benefit from a number of coordinated efforts in sharing information, intelligence, and investigative techniques. For example, UCENet members collectively and actively analyze and disseminate relevant intelligence and information to improve coordination and compliance/enforcement activities among members in a timely manner. With open and trusted lines of communication, enforcement agencies are able to act promptly in identifying risks and opportunities for addressing common challenges at home and abroad.

For those who are already active members of UCENet, benefits can be enhanced through opportunities for ongoing training, contributions to research projects, and displaying leadership in sharing best practices and enforcement lessons with others that may be at the early stages of implementing enforcement actions.

UCENet PILLARS AND PRIORITIES

ENFORCEMENT
To maximise our collective powers and reach to protect citizens, particularly those most vulnerable. To respond to the intelligence and evidence collected in order to detect, disrupt and dissuade criminal and civil breaches of the law and to take appropriate action.

TRAINING
To provide meaningful training for investigators and practitioners at the annual meeting. To explore the desire or need for a consistent training program amongst the UCENet members.

INTELLIGENCE
To collect, analyse and disseminate relevant intelligence or information for the purposes of improving our coordination and compliance/enforcement activities. To act promptly in identifying risks and opportunities and collaborate in addressing common challenges and issues.

3. COMMUNICATIONS
To promote and provide a reliable, safe and efficient method of sharing information and intelligence amongst the UCENet members and with partners, including through the UCENet MOU, to enable delivery of the operational plan. To publicise and promote our compliance and enforcement activities. To promote the advantages of UCENet membership and ensure an understanding of the differing environment of each jurisdiction with the aim of strengthening cooperation and coordination.

Source: www.ucenet.org

CONCLUSION

From nuisance to abuse, unsolicited communications have a wide range of impacts on citizens. Spam is no longer a problem exclusive to email – it has become a vehicle for deceit and has expanded to a multitude of electronic platforms that citizens all over world use to support their businesses, perform their jobs, access government services, and engage in social interactions and relationships. From unknowingly downloading a malware infection to having personal data stolen, bad actors are constantly in search of new victims. Fortunately, many governments see the urgency in acting on these issues, and anti-spam efforts are underway all over the world.

It is critical that governments, regulators, enforcement agencies, and the private sector be aware of these efforts and contribute their knowledge and expertise to build global capacity. These communities must leverage their relationships with each other and ask for assistance when needed, building their own skills and experience that can in turn be shared with others.

While each community may have different priorities and resources, success comes from continuing to work at the intersection of policy, enforcement, technology, and international development. It also requires involving end-users and civil society for the benefit of economic and social prosperity. Sharing information, working alongside partners, and nurturing a network of allies and counterparts are key drivers to moving the anti-spam agenda forward globally.

The next steps outlined in this report represent important collective actions to strengthen enforcement capacity and build robust, flexible policy to combat unsolicited communications. The involvement of the private sector, and the mobilization of global resources like UCENet are also key pillars in advancing our common agenda.

Bringing a group of experts from different communities together for an afternoon of discussion was a good starting point. Fundamentally addressing the challenges associated with spam and unsolicited communications requires dialogue, but more work is needed. Regulators, policy makers, service providers, and enforcement agencies must (i) improve their ability to share information, (ii) learn from one another, and (iii) focus on the common goal of reducing threats to our global communications system. The CRTC looks forward to advancing this dialogue, together with its partners.

APPENDIX A – WORKSHOP AGENDA

IIC 2016 COMMUNICATIONS POLICY & REGULATION WEEK WORKSHOP COMMUNICATIONS SECURITY: COLLABORATING TO ELIMINATE SPAM AND NUISANCE COMMUNICATIONS

Welcome

- **Jean-Pierre Blais**, Chairman and CEO, CRTC

Opening Remarks: Understanding the current landscape

- **Stephen Eckersley**, Head of Enforcement, Information Commissioner's Office, UK

Panel Discussion: ***Cross-border case studies***

Moderator:
- **Chris Chapman**, President, IIC

Speakers:
- **Travis Leblanc**, Chief, Enforcement Bureau, Federal Communications Commission, USA
- **Toni Li**, Assistant Director (Support), Office of the Communications Authority, Hong Kong (Special Administrative Region)
- **Peter Merrigan**, Senior Investigator, Electronic Messaging Compliance Unit, Department of Internal Affairs, New Zealand

Break

Panel Discussion: ***Bridging the gap between policy makers and enforcement agencies***

Moderator:
- **Dr. Steve Unger**, Chief Technology Officer and Group Director for Strategy, International, Technology and Economics & Board Member, OfCom, UK

Speakers:
- **Christine Runnegar**, Director, Security and Privacy Policy, Internet Society
- **Viola Veiderpass**, Digital Crime Officer, Cybercrime Directorate, INTERPOL Global Complex for Innovation

Closing Remarks: *Where do we go from here?*

- **Jean-Pierre Blais**, Chairman and CEO, CRTC
- **Adriana Labardini Inzunza**, Commissioner, Instituto Federal de Telecomunicaciones, Mexico
- **Richard Bean**, Acting Chairman, Australian Communications and Media Authority

CRTC.GC.CA