ANTI-SPAM ACTION

Canada's CRTC and the IIC kicked off discussion on international efforts to combat unwanted communications, as **STEVEN HARROUN** explains

From nuisance to abuse, unsolicited communications encompass 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 across the world.

The Canadian Radio-television and Telecommunications Commission (CRTC), in partnership with the International Institute of Communications (IIC), hosted a workshop on combating spam and other forms of nuisance communications. The half-day event took place as part of the IIC's annual Communications Policy and Regulation Week in Bangkok, Thailand. In attendance were 45 participants – including representatives of regulators from all global regions, and of industry, plus academics and other communications experts.

> **Too often, these conversations take place in isolation... policy may be developed without consideration for enforcement needs.**

The purpose of this workshop was threefold. First, it sought to bring together experts from both policy and enforcement communities around the world, allowing them to exchange views and experiences in policy, regulation, and enforcement of spam and nuisance communications. These 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; policy may be developed without sufficient consideration for enforcement needs, while feedback from investigators may not make its way back to policymakers, resulting in legislative barriers that hinder enforcement activities.

The workshop also had participants brainstorm on how to advance efforts to work collaboratively across borders as the global nature of these issues introduces its own unique challenges. While important considerations for anti-spam efforts can apply to both domestic and international initiatives, the focus of this workshop was primarily international, on approaches to working across jurisdictions.

Finally, these discussions aimed to engage regulators from emerging economies and to introduce them to the work of established networks, communities and organisations working in this space.

SCOPE OF DISCUSSION

The workshop began with a keynote introduction that 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. The first panel, consisting of enforcement experts and practitioners, discussed three case studies, detailing the international and cross-jurisdictional nature of the challenges of enforcing spam and unsolicited communications rules. The second panel, consisting of policy and technical experts, identified capacity gaps and ways to increase harmonisation of cross-border policies and enforcement activities. Discussion also included the opportunities and challenges specific to emerging economies.

WORK IS UNDERWAY

It is critical that governments, regulators, enforcement agencies and the private sector be aware of ongoing efforts and contribute their knowledge and expertise to build global capacity. Each community of expertise 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.

As part of the workshop's introductory keynote, participants were introduced to the Unsolicited Communications Enforcement Network (UCENet), an expert network of organisations engaged in international cooperation on spam enforcement. UCENet coordinates and promotes international cooperation and activities targeting spam related problems such as online fraud and deception, phishing, dissemination of viruses, and unsolicited calls and texts.

In 2016, 11 enforcement agencies, which are also members of UCENet, signed a memorandum of understanding (MoU) to share information and intelligence between agencies. Signatories include the CRTC, ACMA (Australia), the FTC and FCC in the US, the UK's Information Commissioner's Office, the Korea Internet & Security Agency, the Netherlands Authority for Consumers and Markets, the

Department of Internal Affairs in New Zealand and the National Consumer Commission in South Africa.

The organisations have also committed to sharing knowledge and expertise through training programmes and staff exchanges, as well as to inform each other of legal developments in their respective jurisdictions. The MoU provides a clear framework that demonstrates a strong commitment to cross-border cooperation, thereby strengthening the fight against a global problem. Such a development sends a clear message to those responsible for fraudulent or malicious messages and calls: bad actors cannot escape enforcement attention and the interests of citizens are being protected.

This important international agreement allows these agencies to collaborate and pursue cases that cross borders and jurisdictions. Nonetheless, participants at the workshop highlighted continuing challenges caused by legislative and policy inconsistencies. Discussions also touched on the challenges posed by rapid technological evolution facilitating spam and other nuisance communications, and the capacity gaps among nations struggling with these complex issues.

NEW REPORT

Based on these discussions, the CRTC has produced a report that summarises findings from the workshop and outlines agreed actions to improve international collaboration on unsolicited communications. Major themes include:

- **Inconsistencies in policy and legislation:** The global nature of the issue means that cases almost always cross national borders. This can create challenges when policies, approaches and legislative tools are not consistent. These inconsistencies can make it difficult to share information and collaborate on enforcement.
- **Technology enables anonymity:** The rapid evolution of technology has made the job of spammers and fraudsters easier, while rendering effective enforcement more complex. Specifically, VoIP and other OTT applications have allowed spammers to remain anonymous, reduced the cost of sending unsolicited communications around the world, and made it harder to track the proceeds of criminal activities.
- **Capacity building for emerging economies:** While spam and unsolicited communications are a global problem, not all countries are well equipped to combat these threats. Many emerging economies have leapfrogged wireline and gone straight to mobile communications technologies, while lacking a robust legislative framework to control unsolicited calls and emails.

The report elaborates three key 'next steps' that were agreed by workshop participants to advance spam and nuisance communications efforts:

- Engaging in regular policy discussions to ensure that policy and legislation keep pace with the evolution of the threat, including lessons learned from enforcement activities
- Leveraging public-private sector partnerships to ensure clear communication among different agencies involved in fighting unsolicited communications, and tapping the expertise of network operators and other private sector players
- Participating in UCENet to ensure that enforcement agencies collaborate across borders, identify threats and share information.

These next steps represent important collective actions to strengthen enforcement capacity and build robust, flexible policy to combat unsolicited communications. The commitment to continued collaborative discussions, the involvement of the private sector and the mobilisation of global resources like UCENet are key pillars in advancing our common agenda.

Bringing a group of experts from these different communities together for an afternoon of discussions was a good starting point. More work is needed, but fundamentally, addressing this challenge requires dialogue. Regulators, policymakers, service providers and enforcement agencies must improve their ability to share information, learn from one another and focus on the common goal of reducing threats to our global communications system.

We encourage regulators, policymakers and other stakeholders to identify their role in successfully combating this challenge. The CRTC looks forward to advancing this dialogue, together with its partners.

STEVEN HARROUN *is chief compliance and enforcement officer at the Canadian Radio-television and Telecommunications Commission in Ottawa. Visit crtc.gc.ca to download the report.*

MUCH MORE THAN JUST A NUISANCE

- Spam accounts for nearly two-thirds of total email volume, according to Cisco's 2017 annual cybersecurity report, and the company's research suggests that global spam volume is growing due to large and thriving spam-sending 'botnets'. About 8–10% of the global spam observed in 2016 could be classified as malicious, and the percentage of spam with malicious email attachments is increasing. Adversaries appear to be experimenting with a wide range of file types to help their campaigns succeed. See bit.ly/2jtum0w
- Cisco has also addressed a latest spam technique called 'hailstorm', a step on from so-called 'snowshoe' spam campaigns. "Both snowshoe and hailstorm spam are sent using a large number of sender IP addresses, but unlike snowshoe spam, hailstorm campaigns are sent out in very high volume over a short timespan." See bit.ly/2o5q944
- According to the FCC, American consumers received about 29 billion robocalls in 2016 or about 230 calls for every US household. The agency's commissioners have recently voted to adopt rules that allow carriers to block spoofed caller ID numbers associated with phone lines that do not actually dial out, without running afoul of FCC rules requiring carriers to complete all calls. The FCC says unwanted calls are the top concern of consumers. More at fcc.us/2ocVf6B
- Payment fraud involving email addresses sold on the 'dark web' is one of the most common cybercrimes in the UK. In the US, there has been a huge increase in scams targeting tax returns, reports IBM.