Government of Canada Gouvernement du Canada
Canada
Canadian Radio-television and Telecommunications Commission

Enforcement Advisory - Notice for Web Hosting Service Industry

The purpose of this advisory is to promote compliance with Canada's Anti-Spam Legislation (CASL) in the Canadian web hosting space and to increase and publicize CASL outreach activities.

Why web hosting providers?

CASL prohibits sending unsolicited commercial electronic messages (commonly referred to as spam), altering transmission data in electronic messages without consent and installing computer programs without consent. An organization or individual can also be found liable if they provided aid during these activities.

Information gathered by the Canadian Radio-television and Telecommunications Commission (CRTC) shows that malware is being distributed by way of Canadian web hosting infrastructure. Web hosting providers and operators of other networked infrastructure are critical in safeguarding Canadian cyber security.

How are web hosting providers potentially liable under CASL?

While web hosting providers **may** not be directly responsible for violations committed by their clients under sections 6 to 8, they are nevertheless uniquely positioned to detect, prevent and stop these non-compliant activities.

Web hosting providers have obligations under CASL. Specifically, web hosting providers must not behave in any way that contravenes **section 9 of CASL** by aiding, inducing, procuring or causing to be procured acts prohibited by sections 6 to 8.

How can web hosting providers avoid liability?

Organizations and individuals may avoid liability by exercising sound due diligence. Due diligence includes prevention strategies and other safeguards aimed at eliminating or reducing their potential direct or indirect role in contraventions of CASL. This includes the development and implementation of a written corporate compliance program. General guidance and best practices on developing a corporate compliance program can be found in Compliance and Enforcement Information Bulletins CRTC 2014-326 and CRTC 2018-415.

The CRTC recognizes that web hosting providers vary in size, resources, and service offerings. As such, each organization's program will be unique and tailored. However, in all instances, a credible and effective program will include fundamental safeguards to prevent, detect and respond to compliance issues whether detected internally or via alerts received from third-parties.

As detailed in the aforementioned information bulletins, preventative measures may include: Client vetting practices - including identity verification (i.e. – 'know your clients'), a corporate compliance policy, user agreements that include compliance with CASL as a condition for service, and documented standard operating procedures.

Once an organization becomes aware of infected infrastructure, remediating a cyber incident becomes critical to ensuring compliance. This includes both an incident-handling plan and an appropriately resourced incident response team.

Cyber Security References

Anti-abuse and cyber incident response best practices that may serve as useful references in developing your corporate compliance program include:

- The M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers;
- The CCIRC Cyber Incident Management Framework for Canada;
- Spamhaus: "How hosting providers can battle fraudulent sign-ups"; and
- The NIST Computer Security Incident Handling Guide.

Note to cyber-security companies and malware researchers

If you have any information on Canadian infrastructure used for illicit activities (e.g. spam, phishing, malware, or botnet-related activities) and Canadian web hosts which are non-responsive to abuse claims, you can report it to us via email at lcap-casl-inv@crtc.gc.ca.

Date modified:

2018-11-22