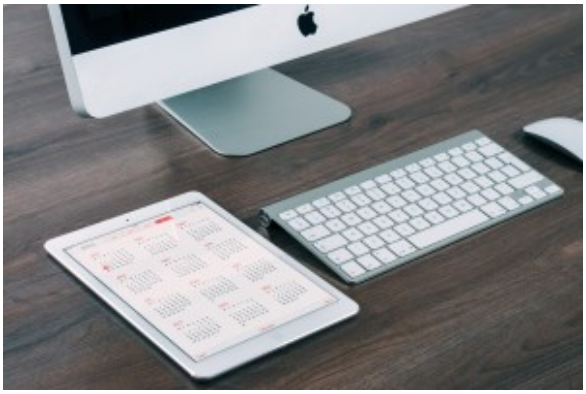
ILN IP Insider

An International Lawyers Network IP Group Publication

# *BOTNET TAKEDOWN: FIRST WARRANT ISSUED UNDER CANADA'S ANTI-SPAM LAW*

***BY MONICA SHARMA OF CLARK WILSON LLP AND KELSEY MARSHALL (ARTICLED STUDENT) OF CLARK WILSON LLP ON DECEMBER 23, 2015***

***POSTED IN CANADA, ONLINE CONTENT***



***Canada's anti-spam law ("CASL") outlines violations, enforcement mechanisms, and penalties aimed at protecting online consumers against spam, electronic threats, and misuse of digital technology. CASL's anti-spam rules came into effect on July 1, 2014. CASL's software update and installation rules came into effect on January 15, 2015. The latter rules are often referred to as malware/spyware computer program rules. Under these rules, CASL applies, in addition to applying in other circumstances, when a person, in the course of a commercial activity, installs or causes to be installed a computer program on any other person's computer system, unless the person has obtained the express consent of the owner or an authorized user of the computer system as required by CASL.***

***The Canadian Radio-television and Telecommunications Commission (the "CRTC") has the primary enforcement responsibility under CASL. Under CASL, the CRTC has various enforcement mechanisms, including obtaining a warrant with respect to a CASL violation. On December 3, 2015, the CRTC announced that it served its first-ever warrant under CASL to take down a command-and-control server located in Toronto, Ontario, which is a centralized computer that issues commands to a botnet and receives reports back from the co-opted computers. A botnet is a set of computers that have been compromised through the installation of malware and which can be instructed to send spam, install additional malicious programs and steal passwords, among other illicit activity.***

***The malware in this case was Win32/Dorkbot malware, which has infected more than one million personal computers worldwide by spreading through social networks, instant messaging programs, and USB flash drives. Once a computer becomes***

*compromised, it can be instructed to: steal passwords used for online banking and payments; download and install dangerous malware; and join other infected computers in sending multiple requests to a specific server in the hopes of overwhelming its capacity to respond (known as distributed denial of service attack).*

*According to the CRTC, agencies from around the world, including the Federal Bureau of Investigation, Europol, Interpol, Microsoft Inc., the Royal Canadian Mounted Police (the "RCMP"), Public Safety Canada, and the Canadian Cyber Incident Response Centre, are working together in the investigation of Dorkbot. The warrant in Canada was granted by a judge of the Ontario Court of Justice and was carried out with assistance from the RCMP. No further details were provided by the CRTC regarding the details of the warrant or the execution process.*

*The ability of the CRTC under CASL to obtain a warrant is quite broad. The CRTC may obtain a warrant authorizing entry to a place, including a dwelling-house, if the justice of the peace is satisfied that entry to the place is necessary to verify compliance with CASL, determine whether CASL has been contravened, or assist an investigation or proceeding in respect of a contravention of foreign state laws that address conduct that is substantially similar to conduct prohibited by CASL. Subject to any conditions specified in the warrant, the person executing the warrant may do the following: examine anything that is found in the place; use any means of communication found in the place or cause it to be used; use or cause to be used any computer system found in the place to examine data contained in, or available to, the system; prepare or cause to be prepared a document based on the data; use or cause to be used any copying equipment to make copies of documents; remove anything found in the place for examination or copying; and prohibit or limit access to all or part of the place.*

*Businesses should be aware that the CRTC has indicated that it will continue to collaborate with its domestic and international partners to aggressively pursue investigations of alleged violations under CASL to protect Canadians from online threats. Although the first warrant under CASL was issued in relation to the installation of malware on computer systems, the software update and installation rules are broad in that they apply to the installation of unwanted software that is not malware or spyware. In order to comply with these rules and to avoid investigation by the CRTC, businesses should seek consent, as required by CASL, prior to installing computer programs on another person's computer system.*

*Executive Offices*
*179 Kinderkamack Road*
*Westwood, NJ 07675*
*Tel: 201.594.9985/ Fax: 201.740.9765*

***London, and Norman Zivin of Cooper & Dunham LLP, New York, New York, the ILN's Intellectual Property Group provides the platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice on cross-border transactions. Members of the group meet regularly at ILN conferences and industry events, and have collaborated on discussions and publications of mutual interest.***

***Read More ❯***