itworldcanada.com

Understanding Canadian Cybersecurity Laws: refactored — our series in summary | IT World Canada Blog

Melissa Lukings and Arash Habibi Lashkari

8-10 minutes

In this tenth and final article in our Understanding Canadian Cybersecurity Laws series, we will look back through the previous nine articles and revisit the topics covered in each of them. Our journey begins with the first article, The Foundations, first published by IT World Canada on January 13, 2020. From there, we'll retrace our journey through our other posts to date.

- Understanding Canadian Cybersecurity Laws: The foundations (Article 1)

  The Foundations (January 13, 2020)

  In our first article, we described and contextualized the foundational structures of the Canadian legal system. We broke down our national legal landscape, providing the basics of sources of law and the jurisdictional division of powers behind our legislation. We explored the areas of statutory law, criminal law, tort law, and common law as they relate to cybersecurity. Finally, we outlined the relevant legislation, including the specific Acts and

statutes which apply to governmental bodies, organizations, and individuals in Canada. >>Read the full article.

- Understanding Canadian Cybersecurity Laws: Privacy and access to information, the Acts (Article 2)

  Privacy and Access to Information, the Acts (February 25, 2020)

  Our second article discussed the federal *Privacy Act*, which establishes the rules for how governmental bodies must operate with respect to the collection, use, retention, distribution, and destruction of personal information collected during operations. We also touch on the *Access to Information Act*, which grants individuals and organizations the right to access, and alter, their own personal information as held by governmental bodies.>>View the article.

- Understanding Canadian Cybersecurity Laws: Privacy protection in the modern marketplace — PIPEDA (Article 3)

  Privacy Protection in the Modern Marketplace — PIPEDA (April 16, 2020)

  This article examined the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and its application to private-sector organizations across Canada that collect, use, or disclose personal information in the course of engaging in commercial activities. We explained how the provisions given in the PIPEDA relate to government, businesses, and individuals. Finally, we discussed the real-world implications of PIPEDA within the evolving landscape of virtual meetings, digital conferences, and online classes brought about by the global COVID-19 pandemic.>>View this article.

- Understanding Canadian Cybersecurity Laws: Interpersonal privacy and cybercrime — Criminal Code of Canada (Article 4)

  Interpersonal Privacy and Cybercrime — Criminal Code of Canada (June 16, 2020)

  The fourth article in our Understanding Canadian Cybersecurity Laws series ventured into the *Criminal Code of Canada*. We defined and discussed the issue of "cybercrime" under the differential labels of cyber-dependent crimes; cyber-enabled crimes; and computer-supported crimes. We further divided these subcategories of crime into specific offences including hacking, possession of "hacking tools," denial-of-service (DoS) attacks, distributed denial of service (DDoS) attacks, botnets, malware, phishing, identity theft and identity fraud, and criminal copyright infringement. Lastly, each subcategory of cybercrime was referenced to the relevant codified provision in the *Criminal Code of Canada*.>>View this article.

- Understanding Canadian Cybersecurity Laws: 'Insert something clever here' — Canada's Anti-Spam Legislation (Article 5)

  "Insert Something Clever Here" — Canada's Anti-Spam Legislation (August 3, 2020)

  Our fifth article spotlighted *Canada's Anti-Spam Legislation* ("CASL"), first by defining and contextualizing "spam," then exploring attacks such as remote code execution (RCE), remote access Trojan (RAT), and large-scale spamming botnet attacks. We rounded off the article by discussing the express consent requirements for commercial electronic messages (CEMs), the parties to whom this law applies, the exemptions to the CASL requirements, and the issue of commercial non-compliance.

>>View this article.

- Understanding Canadian Cybersecurity Laws: Peer-to-peer privacy protection — 'Intrusion Upon Seclusion' and the Protection of Intimate Images (Article 6)

  Peer-to-Peer Privacy Protection — "Intrusion Upon Seclusion" and the Protection of Intimate Images (October 9, 2020)

  In the sixth article of our Understanding Canadian Cybersecurity Laws series, we highlighted the relatively "new" common law privacy tort of "intrusion upon seclusion," which was recognized in the Ontario case of *Jones v. Tsige* (2012 ONCA 32), and provides victims of certain privacy breaches the ability to sue the invasive party in civil court. We also discussed the relatively new criminal offences relating to cyberbullying and the illegal distribution of intimate images, which were created by the *Protecting Canadians from Online Crime Act,* following the highly-publicized Canadian suicide deaths — both of which were linked to cases of extreme cyberbullying. >>View this article.

- Understanding Canadian Cybersecurity Laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)

  Deep, Dark and unDetectable — Canadian Jurisdictional Considerations in Global Encrypted Networks (November 20, 2020)

  Our seventh article explored the cross-jurisdictional nature of the DarkWeb and DarkNet. We started out by categorizing online content as being either "Surface Web", "Deep Web", or "Dark Web" content, providing a basic overview for the not-so-technologically-