

THE OSGOODE CERTIFICATE IN PRIVACY & CYBERSECURITY LAW

Course starts February 24, 2021
5 days over 5 weeks • Online only

Privacy and cybersecurity law is an increasingly complex and high stakes area of practice.

It is imperative that all professionals – and their advisors – treat data privacy and cybersecurity as a priority; not as an afterthought.

You need to be prepared and know how to respond. Quickly.

Over the course of **5 online modules**, get the practical knowledge and skills you need to respond to new and unexpected privacy and cybersecurity incidents.

Focused on **practical, real-world scenarios**, you will **'learn-by-doing'** and get **individualized feedback**. You will:

- Perform a risk assessment
- Respond to a data breach
- Learn how to develop privacy policies, processes, and internal controls
- Analyze legal requirements and develop a compliance plan

Program Director

Amy ter Haar, LL.B., LL.M.
Osgoode Professional
Development

Format

Online – Interactive

*You will have online access
to the program for 120 days.*

Register today at:

[osgoodepd.ca/
cyber-cert](https://osgoodepd.ca/cyber-cert)



*This program has been pre-approved
by the International Association of
Privacy Professionals (IAPP) and is
eligible for 12 CPE credits.*



The Osgoode Certificate in Privacy & Cybersecurity Law

Benefits of the Program:

- Curriculum and resources were specifically **designed** for learning online
- **Learn at your own pace**, with **120-day** access to the program archive
- Weekly live, **interactive online sessions** with industry experts and other learners
- **Hands-on learning in simulations** with peers, including **1:1 feedback** from the faculty and Program Director
- Weekly, **'virtual office hours'** with Program Director to clarify any questions or concerns
- An **online forum** to interact with faculty and other learners so you can reflect on course content and build your professional network
- Obtain an **Osgoode Certificate in Privacy and Cybersecurity Law** upon completion of online modules, exercises and obtaining a passing grade on the online multiple choice exam.

The Osgoode Certificate in Privacy & Cybersecurity Law is an intensive and unique online offering that will give you a competitive edge and the critical knowledge and skills to stay ahead of the complicated and porous scheme of legal privacy protections governing online and offline individual information in Canada.

Designed to meet the needs of working professionals, the certificate is delivered in a dynamic and engaging virtual classroom. Each week of the 5 week program, you will have access to recordings, resources and exercises that explore the key legal and policy issues related to privacy and cybersecurity.

The course will give you a practical overview of effective strategies to protect information, including tactics for responding to privacy and cybersecurity challenges.

Our innovative format fosters interaction among students and our outstanding faculty. Through a combination of focused online discussions and participation in real-world exercises, you will actively engage with critical concepts from key industries and sectors.

Register today at:

osgoodepd.ca/cyber-cert



In addition to engaging in practical, real-world 'learn-by-doing' exercises, you will:

- Learn how to confidently navigate data privacy laws and manage data privacy risks
- Develop best practices for ensuring resilience against cyberattacks
- Recognize the relationship between privacy, cybersecurity and risk management across various industry sectors
- Draft privacy policies and understand the role and importance of these
- Identify and manage risks associated with the collection, use and disclosure of business and personal information
- Apply the European Union's General Data Protection Regulation (GDPR) to different business practices and technologies
- Discuss future directions in the evolution of data protection and information privacy law
- Assess potential legal liability stemming from privacy and security breaches and design appropriate responses
- Evaluate the current Canadian legal framework for consumer privacy protection
- Identify the key sources of law applicable to the internet as a decentered, community-standards focused network system
- Understand the role of tort lawsuits for individual consumer privacy violations

Who Should Attend

- Lawyers interested or advising on privacy & cybersecurity
- In-house counsel
- Government and regulatory counsel or representatives
- Privacy, information, security and technology officers
- Compliance and risk management professionals
- Professionals in a managerial, executive or director position looking to increase their knowledge in privacy & cybersecurity
- Consultants in IT or privacy & cybersecurity

You will learn and gain tremendous insight from a faculty of leading privacy and legal experts, including:

Program Director



Amy ter Haar,
LL.B., LL.M.

Osgoode Professional Development

Advisory Board

Imran Ahmad

Partner, Blake, Cassels & Graydon LLP

Karen Burke

Privacy & Data Innovation Expert

Lyndsay Wasser

Co-Chair, Privacy & Data Protection,
McMillan LLP

Éloïse Gratton

Partner & National Co-Leader of the
Privacy & Data Protection Practice
Group, Borden, Ladner Gervais LLP

Supporting Faculty

Catherine Beagan Flood

Partner, Blake, Cassels & Graydon LLP

Matthew Davies

Senior Underwriting Specialist,
Chubb Canada

David Goodis

Assistant Commissioner, Information and
Privacy Commissioner of Ontario

Lynn Larson

Senior Counsel, BCE Inc.

Vance Lockton

Manager, Digital Governance,
Waterfront Toronto

Daniel Michaluk

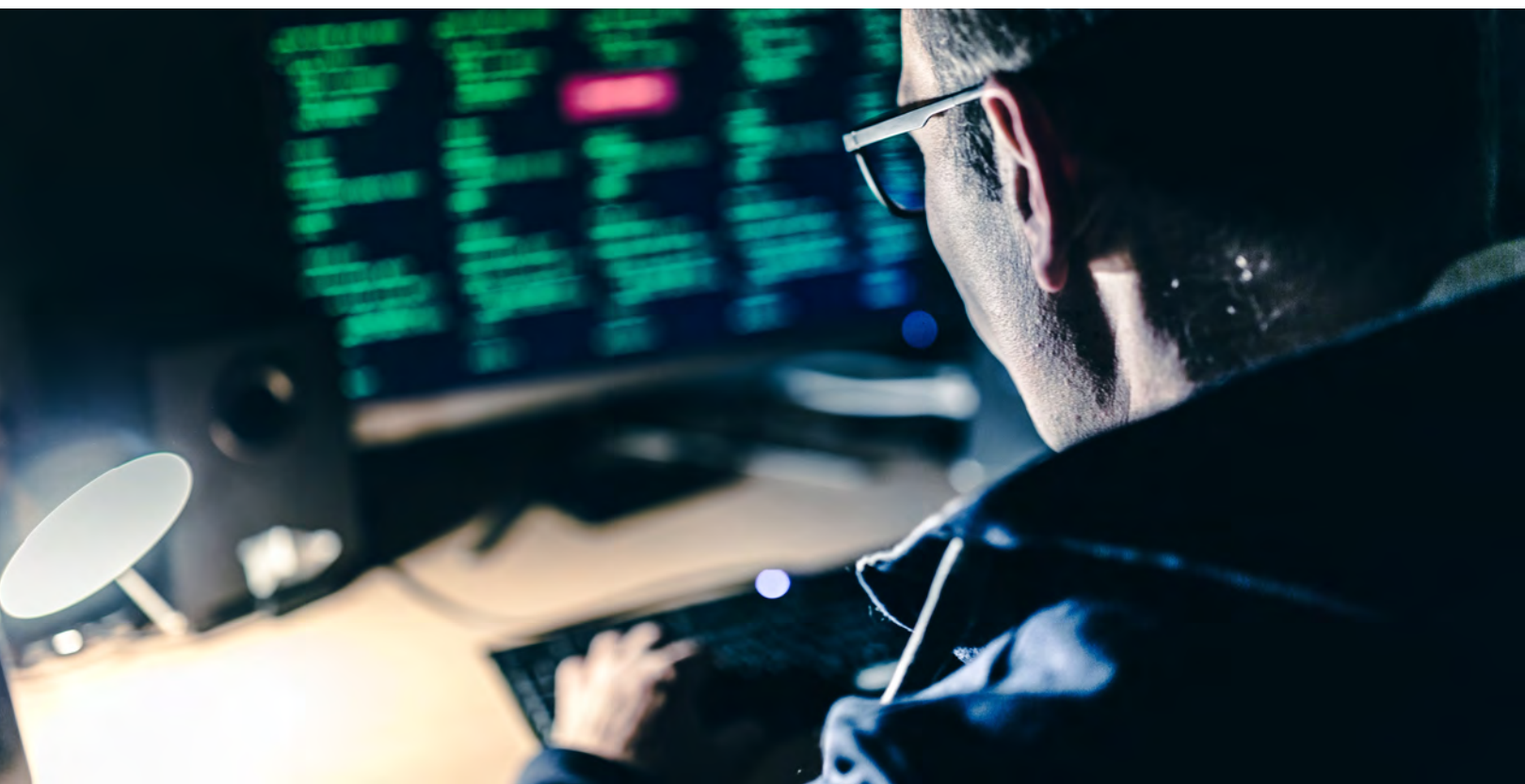
Partner, Borden Ladner Gervais LLP

Andrea Slane

Associate Dean, Research and Graduate
Programs, Ontario Tech University

Register today at:

[osgoodepd.ca/
cyber-cert](https://osgoodepd.ca/cyber-cert)



Agenda

WEEK 1

Foundations and Themes of Canadian Privacy Law

Privacy laws are based on a conception of privacy, which informs what the law protects. In this opening module, we provide a broad overview of privacy law to understand the key issues involved. The focus is to provide a sound understanding of basic privacy concepts, so you can answer what is privacy, how do privacy laws work and what do privacy laws protect.

- Introduction to the institutions that make and apply privacy law
- The relationship and differences between international privacy law cultures
- Types of social trends and technological challenges that affect privacy law
- Social and ethical issues that are relevant to privacy law
- Evolution of privacy law, including enforcement of the law and how courts and legislators have interpreted privacy harm
- Recognize the difference between personal and enterprise data, how to protect it and assess organizational privacy concerns
- Understand an organization's responsibilities when collecting, processing, and using personal data within and across borders

WEEK 2

Frameworks of Global Privacy and Data Protection Law

In this module, the focus is on key concepts of privacy common across international jurisdictions. It explains areas where approaches to privacy both converge and diverge to help you generate strategies when responding to global privacy concerns at an organizational level.

- Assess and compare common privacy law regimes and cultures from select areas around the world, and explore how these laws balance privacy with the public interest. Lessons are focused on the following:
- European Union's General Data Protection Regulation (GDPR)
- Organization for Economic Cooperation and Development (OECD) Privacy Guidelines, and
- The nine principles of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework
- Understand and conduct Privacy Impact Assessment, Data Protection Impact Assessment, and Legitimate Interest Assessments

WEEK 3

Laws Governing Data Use and Data Disclosure

This module provides a synthesis of the sprawling landscape of privacy laws and regulations. It discusses the current state of freedom of information rights and limitations and how the law is evolving to keep up with today's digital society.

- The accommodation of commercial interests for outsourcing and cloud services, and the evolving debate over the monetization of data and its consumer protection and competition law aspects
- Identify, formulate and critically explore how data information laws balance privacy rights with the public interest
- How consumer protection and competition/anti-trust laws are evolving to protect consumers from unfair practices, price discrimination, and anti-competitive data hoarding. How criminal laws, national security laws, the Charter of Rights and Freedoms regulate the use of data and compelled disclosure of data by governmental agencies and private enterprises – both compelled circumstances and public interest
- Understand the purpose of anonymizing data and dive into how to practically anonymize data from the perspectives of governments and organizations

- Explore the practical challenges of anonymizing data and strategies for overcoming these challenges

WEEK 4

Law of Confidential Information, Privacy and Access

Using active learning activities, this module provides you with necessary skills to design and deliver effective privacy and information management programs and procedures. Emphasis is placed on the importance of vigilance surrounding privacy protection, data security, and risk management, so you can develop practical skills to improve cybersecurity and minimize risk and data breaches.

- Distinctions in how the law of confidential information is distinct from other legal regimes protecting personal or proprietary information
- Classifying information, including confidentiality re: professional obligations, trusts, and data custodians
- Contractual obligations of confidentiality (i.e. non-disclosure agreements etc.)
- The overlap and divergence between privacy and confidentiality
- Solutions to access government information containing confidential information and access to public interest disclosure of confidential information (e.g. whistleblowers)

WEEK 5

Privacy Breach Readiness & Resilience: Legal Obligations

Module 5 equips you with the core competencies to devise and implement policies & practices required by data protection laws and ensure compliance in a cost effective and productive manner. It uses the most recent real cases and scenario analysis, including relevant discussion around previously imposed legal penalties, fines, business limitations, and licence revocations.

- The evolution of cybersecurity law
- The main cybersecurity issues courts and legislators face
- Enforcement of cybersecurity law
- Identifying and protecting personal and enterprise data
- Cybersecurity and data breach insurance
- Responding to data breaches from legal and business perspectives

Register today at:

[osgoodepd.ca/
cyber-cert](https://osgoodepd.ca/cyber-cert)



Registration Details

Fee per Delegate: \$2,995 plus HST

Governmental Delegates: \$2,495 plus HST

Newly Licensed Delegates (2017 – Present): \$1,500 plus HST

Fees include attendance, electronic materials, technical support and 120-day access to program archives. Visit www.osgoodepd.ca/financial-assistance for details about financial assistance.

Program Changes

We will make every effort to present the program as advertised, but it may be necessary to change the date, location, speakers or content with little or no notice. In the event of program cancellation, York University's and Osgoode Hall Law School's liability is limited to reimbursement of paid fees.

Cancellations and Substitutions


Substitution of registrants is permitted at any time. If you are unable to find a substitute, a full refund is available if a cancellation request is received in writing 21 days prior to the program date. If a cancellation request is made with less than 21 days notice, a \$150 administration fee will apply. No other refund is available.

For Further Program-Related Information, Please Contact:


Amy ter Haar, Program Director at 647-527-3996
or email aterhaar@osgoode.yorku.ca

4 Convenient Ways to Register

 osgoodepd.ca/cyber-cert

 416-597-9724

 osgoodepd@osgoode.yorku.ca

 416-597-9736



OsgoodePD has been approved as an Accredited Provider of Professionalism Content by the LSO.

Eligible CPD Hours – LSO (ON): 32h 30m CPD (23h 30m Substantive; 8h 45m Professionalism; 15m EDI)



This program is approved for LAWPRO Risk Management Credit.



This program has been pre-approved by the International Association of Privacy Professionals (IAPP) and is eligible for 12 CPE credits.

OsgoodePD programs may be eligible for CPD/MCLE credits in other Canadian and US jurisdictions. To inquire about credit eligibility, please contact: cpd@osgoode.yorku.ca.

Certificate of Program Completion

In order to be issued the **Osgoode Certificate in Privacy & Cybersecurity Law**, all learners must complete all five online modules. This includes viewing micro-lessons, participating in online group discussion and completing all assignments. Assignments will be a blend of individual and group work. Throughout the course, learners will engage in peer learning and review. Participation is an important component of their learning assessment throughout.

A final online exam must be completed within 30-days of the last module. Learners must obtain an 80% grade.