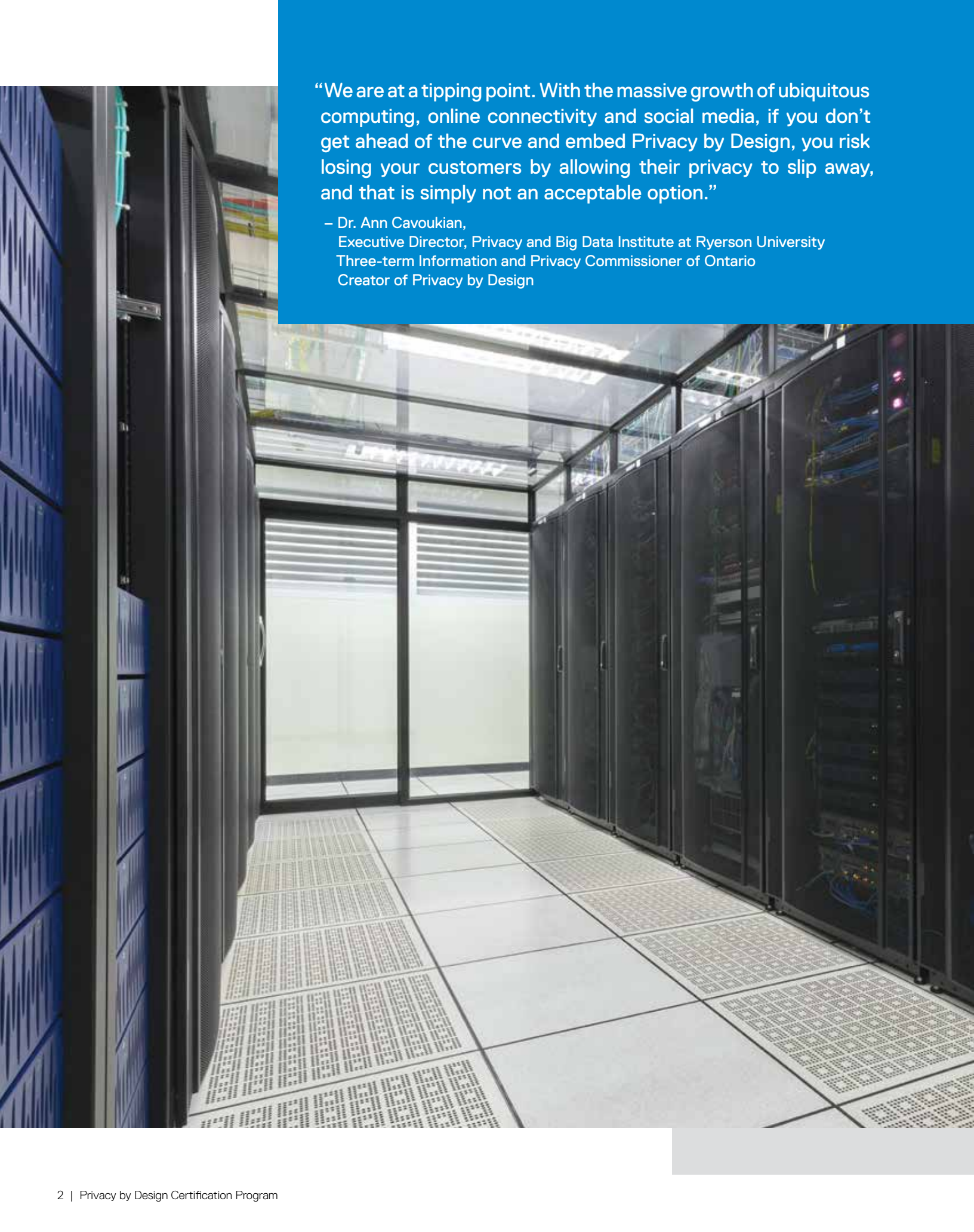# Commit to Privacy, Publicly

Privacy by Design Certification Program
Ann Cavoukian, Ph.D.

Ryerson University

Privacy & Big Data Institute

CERTIFIED

P BY D

RYERSON UNIVERSITY

Privacy Certified by Design

"We are at a tipping point. With the massive growth of ubiquitous computing, online connectivity and social media, if you don't get ahead of the curve and embed Privacy by Design, you risk losing your customers by allowing their privacy to slip away, and that is simply not an acceptable option."

– Dr. Ann Cavoukian,
  Executive Director, Privacy and Big Data Institute at Ryerson University
  Three-term Information and Privacy Commissioner of Ontario
  Creator of Privacy by Design

Strive for Privacy by Design Certification

Earning PbD certification begins at Ryerson

Data breaches are no longer the exception – they have become the norm. One of the largest banks in the United States had its database compromised with the names and contact information of 75 million customers stolen. In another similar incident, 56 million customers had their credit card information siphoned after one of North America's largest retailers suffered a malware attack.

These types of attacks aren't necessarily initiated on home soil. In the Internet age, they may originate from anywhere in the world, at any time. It is no wonder then, now more than ever, that privacy-conscious consumers want to feel confident that the companies and institutions they entrust with their personal data will manage it with the utmost care. Earning Privacy by Design Certification from the Privacy and Big Data Institute at Ryerson University will enhance consumer confidence and trust.

The Privacy and Big Data Institute at Ryerson University is a leader in the research, education and development of big data solutions that will allow organizations to maximize the potential of big data while ensuring that people's privacy is strongly protected.

Our Privacy by Design Certification is the first-of-its kind privacy certification that is based on Privacy by Design, a revolutionary privacy framework that has been recognized globally and translated into 37 languages.

The certification process we follow brings together a framework created by Dr. Ann Cavoukian, one of the world's leading privacy experts, three-term Privacy Commissioner of Ontario, and now the Executive Director of the Privacy and Big Data Institute at Ryerson University. Dr. Cavoukian's approach seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices. We then marry this approach by partnering with the expertise of Deloitte, whose global data protection and privacy practice is comprised of multi-disciplinary professionals specializing in technology, policy, security, law, information governance and management, project management, communications, and privacy regulatory affairs.

Deloitte operationalized the 7 Foundational Principles by developing 29 measurable privacy criteria and 109 illustrative privacy controls using a unique scorecard approach that aligns to Privacy by Design. The criteria and controls are based on key requirements derived from national and international privacy regulations and best practices. (ryerson.ca/pbd/certification)

Most impressive, when you earn Privacy by Design Certification from the Privacy and Big Data Institute at Ryerson, you'll be raising the bar and meeting a privacy standard that is now recognized in more than 35 countries. Doing so will enable you to gain a competitive advantage over other organizations, which is sustainable over time.

"Privacy should not be a one-time compliance exercise. We help our clients innovate and expand their digital footprint by using a risk-based approach to implementing new technologies."

– Sylvia Kingsmill, BA, LLB, National Partner,
  Digital Privacy Leader at Deloitte

Achieve the highest level of privacy

In October 2010, regulators at the International Conference of Data Protection Authorities and Privacy Commissioners unanimously passed a resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. By qualifying for Privacy by Design Certification, your organization will gain the ability to:

• Enhance compliance by getting ahead of the legislative curve and minimizing compliance risk.

• Reduce the likelihood of fines and penalties, including financial losses and/or liability associated with privacy breaches.

• Build your brand by fostering greater consumer confidence and trust, thereby gaining a sustainable, competitive advantage.

• Better manage post-breach incidents to regain consumer trust and confidence.

• Maintain best practices by seeking independent testing of privacy and security controls, which greatly exceeds the "trust-me" model of self-reporting.

Examine your privacy practices

Ryerson's Privacy and Big Data Institute is collaborating with a global team of Deloitte privacy and information security professionals who will put your organization through a three-step process in order to achieve Privacy by Design Certification.

Step 1: Apply

Applications for certification may be initiated by applying online via Ryerson's website. (ryerson.ca/pbd/certification)

Step 2: Assess

Using a set of well-defined assessment criteria, Deloitte's privacy and security professionals will test your product, service or offering against the 7 Foundational Principles of Privacy by Design.

An assessment of the strength of your privacy practices will be conducted, following internationally-recognized privacy principles, including privacy regulations, industry self-regulatory requirements and industry best practices (e.g., FIPs, OECD, GAPP, CBR and APEC Privacy Framework) using an assessment methodology based on harmonized privacy and security requirements.

Taking a holistic and risk-based approach, Deloitte will test your controls using a quantifiable scorecard.

Step 3: Certify

Upon review of the assessment report, certification will be granted only when Ryerson is satisfied that no significant gaps exist as identified by Deloitte in the Privacy Scorecard.

"Taking a comprehensive, risk-based approach to data privacy — where globally-defined risks are anticipated and counter-measures are built into systems and operations, by design — can be far more effective, and more likely to meet the various requirements of multiple jurisdictions."

– Dr. Ann Cavoukian

7 Foundational Principles of Privacy by Design

1 **Proactive not reactive — Preventative not remedial**
The Privacy by Design (PbD) framework is characterized by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to identify the risks and prevent the harms from arising. In short, Privacy by Design comes before the fact, not after.

2 **Lead with privacy as the default setting**
We can all be certain of one thing — the default rules. Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice as the default. If individuals do nothing, their privacy still remains intact. No action is required on the part of individuals in order to protect their privacy — it is already built into the system by default.

3 **Embed privacy into design**
Privacy measures are embedded into the design and architecture of IT systems and business practices. These are not bolted on as add-ons after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system without diminishing functionality.

4 **Retain full functionality (positive-sum, not zero-sum)**
Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through the dated, zero-sum (either/or) approach where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both.

5 **Ensure end-to-end security**
Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy from start to finish. This ensures that all data are securely collected, used, retained and then securely destroyed at the end of the process in a timely fashion. Thus, Privacy by Design ensures cradle to grave secure lifecycle management of information, end-to-end.

6 **Maintain visibility and transparency – Keep it open**
Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact operating according to the stated promises and objectives, subject to independent verification. The data subject is made fully aware of the personal data being collected and for what purposes. All the component parts and operations remain visible and transparent to users and providers alike. Remember, trust but verify.

7 **Respect user privacy – Keep it user-centric**
Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options. The goal is to ensure user-centred privacy in an increasingly connected world.

Prove to your customers that privacy is one of the highest priorities for your organization.

Become Privacy by Design-Certified today.

About Dr. Ann Cavoukian

Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She is presently the Executive Director of the Privacy and Big Data Institute at Ryerson University. Appointed as the Information and Privacy Commissioner of Ontario, Canada in 1997, Dr. Cavoukian served an unprecedented three terms as Commissioner. There she created Privacy by Design, a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and accountable business practices, thereby achieving the strongest protection possible. In October 2010, regulators at the International Conference of Data Protection Authorities and Privacy Commissioners unanimously passed a resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. Since then, Privacy by Design has been translated into 37 languages. Dr. Cavoukian was chosen as one of the "Power 50" by Canadian Business magazine for her tireless efforts as a privacy champion. She was also selected for Maclean's Magazine's "Power List" of the top 50 Canadians, and was chosen as one of the top 10 women in data security, compliance and privacy to follow on Twitter.

About Ryerson University and the Privacy and Big Data Institute

Ryerson is Canada's leader in innovative, career-focused education. It is a distinctly urban university with a focus on innovation and entrepreneurship. Ryerson has a mission to serve societal need and a long-standing commitment to engaging its community. The Privacy and Big Data Institute at Ryerson was created to serve as a hub for Ryerson faculty, staff and students engaged in data-driven research, innovation and education. The institute's mission is to pursue and promote collaborations with industry to address privacy, security and data analytics challenges.

To learn more, visit **ryerson.ca/pbd/certification**
or contact:
Dr. Ann Cavoukian
Executive Director, Privacy and Big Data Institute
ann.cavoukian@ryerson.ca