



# Youth Online: Beware of the “5 Ps” When Using Social Networks

**Presented by Ann Cavoukian, Ph.D.**

Information & Privacy Commissioner,  
Ontario, Canada

**at the 31<sup>st</sup> International Conference of Data Protection and Privacy Commissioners**

For young people today, going online to connect and interact with others is a natural and integral part of daily life. As they log on to email, blog, chat, or participate in online social networks, young people no longer see the Internet as simply a tool, but rather as an extension of their social lives and public identities.

While most cyber experiences are extremely positive, many young people appear to go on “auto-pilot” when they are online, not thinking twice about broadcasting intimate details about themselves on various websites. Regrettably, this has resulted in abuses and unanticipated consequences ranging from cyberbullying, identity theft, and stalking, to school expulsions and future job prospects being ruined by indiscretions posted online.

While many young people are aware of the possibility of physical threats arising from Internet activities, such as those posed by cyber predators, few fully understand the range of additional risks associated with posting too much personal information online. Most are not conscious that information can remain in cyberspace virtually forever, and can be viewed, copied and downloaded by millions of people. As a result, the personal details they share today can be used to embarrass, hurt or stigmatize them at a later date. Similarly, their online activities can be used covertly for marketing or commercial purposes.

The Office of the Information and Privacy Commissioner of Ontario (IPC) is mandated to build public awareness about Ontario’s access to information and privacy laws. Since 2006, when social networking sites first began making headlines as a technological and social phenomenon, the IPC has made it a priority to educate the public, stakeholders, operators of websites, and especially young people about their shared responsibility to protect personal information online.

The focus of our message to young people has been that they need to be proactive and to think before they post. Nothing is ever deleted from the Internet. So we’ve encouraged them to consider that the “5 Ps” (Predators, Parents, Professors (teachers), Prospective Employers and Police) can view their postings online and to think about whether they are comfortable with the information they are sharing. We teach them that privacy is about freedom of choice and that they can control how much personal information they post online and who is granted access to it.

We've used a variety of channels to reach out to youth. These include school programs, media, conferences, and partnerships with organizations that work closely with young people. We've also participated in helping to form an innovative peer-to-peer network to build awareness among youth.

At the same time, we've also worked closely with key stakeholders, like Facebook and MySpace executives, who have the capacity to make privacy enhancing options available to users and to spread the word about using those options to make choices about how much personal information to share online and with whom.

The IPC is part of a global community of Privacy Commissioners and Data Protection Authorities that are drawing attention to the pressing need to engage young people in managing the risks associated with their online activities. With our international counterparts, we've been gathering momentum behind this issue, from all parts of the world.

As we look ahead to further opportunities to enhance awareness about the privacy challenges that youth face on the Internet, it is useful to reflect back on our achievements to date, and to explore how the various channels used have contributed to supporting our educational goals.

## 1. Engaging Social Networking Websites

### Facebook

In 2005, as Facebook was preparing to open its website to the general public, senior executives approached the IPC seeking our input on their privacy measures. We recognized immediately that collaborating with Facebook was a great opportunity to improve the range of privacy controls available to users and to increase awareness about exercising those options.

Since Facebook was still relatively new to the Internet, our first step was to develop a better understanding of the perspective of Facebook's core users - students and youth. In August 2006, the IPC convened a focus group of eighteen university students from Ryerson University, Queen's University, the University of British Columbia, George Brown College, the University of Toronto and York University, to discuss online social networking.

The group's feedback was illuminating. Almost all of the students were active users of Facebook and strongly favoured it. Most were completely unaware of any potential privacy issues, had not read the website's privacy policies, and did not know anything about the privacy filters available for their use. It was clear that more education in this area was urgently required.

Since then, Facebook and other social networking websites have exploded in popularity and are obviously here to stay. More than ever, it is critical to build awareness among young people about the importance of exercising good judgment when using social networking websites. To address this need, the IPC produced several resources aimed specifically at Facebook users:

- In October 2006, the IPC and Facebook released a joint brochure, *When Online Gets Out of Line: Privacy – Make an Informed Online Choice*, which encourages university, college and high school students to carefully consider their privacy options before posting their personal information online.

- In May 2007, the IPC released *How to Protect your Privacy on Facebook*, a tip sheet which outlines detailed steps on how to set privacy settings on Facebook to the optimal level of protection. The tip sheet was updated in 2008.
- In October 2007, the IPC produced another tip sheet, *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*, which warns Facebook users that information they post on their profile can be searched by current and prospective employers.
- In July 2008, Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, and Chris Kelly, Chief Privacy Officer of Facebook, produced a DVD, *Be a Player: Take Control of Your Privacy on Facebook*, which provides step-by-step instructions on how to use the privacy settings on Facebook.

The IPC's excellent working relationship with Facebook has allowed us to influence the site's privacy practices as they evolve over time. In December 2007, for example, the IPC wrote to Facebook to express strong concerns about its new *Beacon* ad service program. Beacon, which ultimately stirred great controversy among Facebook users, tracks subscribers' activities on external partner websites and publishes this information on news feeds that can be viewed by the subscriber's social network. The tracking continues even when users have logged-off of Facebook and declined to have their activities published on news feeds.

As a result of the IPC's intervention and the criticism of other privacy advocates and users, Facebook eventually decided to offer its users the choice to opt out of Beacon altogether.

The IPC strongly believes that building collaborative relationships with website operators such as Facebook puts us in a better position to influence how privacy safeguards are shaped and delivered and to inform users about their privacy choices.

## 2. Education and Outreach

### Teacher's Guides

The IPC has been working to educate students about open government and privacy within the school system for several years, evolving a variety of resources that support deeper awareness and understanding. Our elementary and secondary school program: *What Students Need to Know about Freedom of Information and Protection of Privacy* is designed for students in grades 5, 10, 11 and 12. It provides guidance to teachers on delivering classes and activities that focus on the concepts of freedom of information and personal privacy.

In 2008, we updated the grade 10 teacher's guide to include a module about online social networking. The module focuses on the potential privacy implications of posting personal information to a social networking site, and helps students understand the options they have to limit who has access to information about them.

### iCommish

In October 2007, Dr. Ann Cavoukian participated in *The Revealed "I": A Conference on Privacy and Identity* hosted by prominent privacy researchers at the University of Ottawa. The conference brought together research talent and experts from academic, public, private, and not-for-profit sectors to discuss the impact of information and authentication technologies on identity.

For the purposes of the conference, the Commissioner, along with the privacy commissioners of Alberta and British Columbia, was asked to create a Facebook profile and live a “second life” on Facebook over the summer of 2007. The commissioners were then asked to discuss the results of their group experiment at the conference on a panel called “iCommish.” Dr. Cavoukian offered her tips for keeping Facebook profiles as private as possible, and expressed concerns, shared by the other commissioners, that personal information posted on Facebook could be easily accessed and used for purposes other than social networking (i.e. harassment, stalking, law enforcement, employer checks, etc.). The panel generated interesting and lively discussion that highlighted the risks associated with social networking sites, but also identified the value of Facebook as a means of expressing identities online.

## School Outreach

As part of its outreach activities, the IPC visits elementary and secondary schools to speak directly to students about the privacy risks inherent in online activities. The focus is on helping students to understand their responsibility to protect their own online privacy, and on helping them understand the options available to help them do this. In our experience, these face-to-face meetings are highly effective.

We’ve visited a number of schools, including Havergal College, The York School and Earl Grey Senior Public School. Sometimes the focus is quite specific. For example, in December 2006, the Commissioner was invited to speak to students and parents at Toronto’s Bishop Strachan School, which was experiencing troubling incidents of cyberbullying in social networking sites and email. Following the presentation to the students, the Commissioner met separately with parents, most of whom were unfamiliar with cyberbullying and other risks that online technologies present.

## Media Interviews

The media has an important role to play in raising public awareness of issues associated with social networking sites. The IPC regularly makes itself available for media interviews, providing tips about online privacy protection and highlighting its extensive information resources.

## Youth Privacy Online: Take Control, Make It Your Choice!

Conferences provide good opportunities to build awareness about online privacy issues and explore possible solutions.

In September 2008, the IPC hosted a conference in Toronto entitled *Youth Privacy Online: Take Control, Make It Your Choice!* The conference focused on the privacy risks that young people are exposed to when they use online communication tools, and looked at various methods of safeguarding personal information online.

Speakers included recognized leaders in the fields of research, education, parent advocacy and technology. Opening remarks were made by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, the Honourable Kathleen Wynne, Ontario Minister of Education, and Parry Aftab, well-known Internet safety advocate and lawyer. Presentations were also made by several Canadian researchers, representatives from the education sector, and technology representatives from Facebook, Microsoft and Research in Motion. A rousing keynote address was delivered by Barbara Coloroso, internationally renowned parent advocate and author. She gave the audience entertaining and insightful advice about teaching children to think critically and ethically when faced with challenging situations.



Conference participants came away with a clearer understanding of the role that online social networking plays in the lives of young people, helping them learn, collaborate, and empower themselves. They also learned that youth may have a unique perspective on online privacy that permits open sharing of personal information within defined networks. While participants shared a sense that technology solutions will continue to evolve, providing better safeguards for personal information online, it was clear to all that these solutions will never take the place of sound judgement and effective parental guidance.

The conference proved to be a valuable learning opportunity for both speakers and participants, and sparked considerable media interest. It was an important step in focussing on the unique issues faced by young people in the online world.

## Teenangels

Peer-to-peer models for spreading the message about privacy to young people hold tremendous potential. Youth often see their peers as more credible sources of information, and may be more motivated to learn from them than from other authority figures.

That's why, in 2008, the IPC helped form the first Toronto Chapter of Teenangels. Founded by Parry Aftab, well-known cyber lawyer and Executive Director of WiredSafety.org, Teenangels is a charitable program that trains 13-18 year old volunteers to educate other teens, younger kids, parents and teachers about online safety, privacy and security.

In the course of their training, members of Teenangels participated in the IPC's conference *Youth Privacy Online: Take Control, Make It Your Choice!* and helped deliver workshops on online privacy and cyberbullying to students.

## Bacchus Canada

In trying to reach out to young people, the IPC recognizes the value in working together with organizations that have a similar issue in youth and youth issues. In September 2008, Bacchus Canada asked Commissioner Cavoukian to tape a public message for their student awareness campaign on online social networking.

Bacchus Canada, a division of The Student Life Education Company, is a non-profit organization that seeks to promote healthy decisions about alcohol and other health issues among post-secondary students.

Dr. Cavoukian's video message, which has been posted on Bacchus Canada's Facebook page, urges viewers to be proactive about protecting their privacy online, and to educate themselves about the privacy controls available on social networking websites.

### 3. National and International Initiatives

#### Resolutions on Children's Online Privacy

On June 4, 2008, the IPC joined its counterparts across Canada in endorsing a *Resolution on Children's Online Privacy*. The Resolution, among other things, calls upon Canada's privacy commissioners to work collaboratively on developing and promoting education-based activities, pressing industry to adopt strong privacy standards and urging operators of websites to implement better privacy practices.

On October 17, 2008, at the 30<sup>th</sup> International Conference of Data Protection and Privacy Commissioners in Strasbourg, France, the IPC and other data protection authorities from around the world endorsed a similar *Resolution on Children's Online Privacy*. Like the Canadian version, the Resolution strongly urges data protection authorities to support collaborative, education-based approaches and to encourage operators of websites to adopt privacy-protective policies and measures.

The IPC is committed to the principles set out in the Resolutions, and is pleased that, through its extensive outreach activities, the IPC is already on track to meet or exceed the stated goals. The IPC looks forward to working collaboratively with other data protection authorities to advance knowledge and education in the area of youth online privacy.

#### Report and Guidance on Privacy in Social Network Services

The privacy and security issues associated with online communities are a matter of global concern. As a member of the International Working Group on Data Protection in Telecommunications, the IPC helped to inform the development of the *Report and Guidance on Privacy in Social Network Services* ("Rome Memorandum"), which was released on March 4, 2008. The Working Group was initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media.

The Rome Memorandum includes a comprehensive list of the known privacy risks associated with the use of social networking sites and guidance on privacy-protective measures for regulators, providers and users of social networking sites. It is an important resource for the public and stakeholders on best practices for safeguarding personal information on social networking sites.

### 4. SmartPrivacy: The Future of Privacy

The future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, "privacy" – which is the cornerstone of all our rights and freedoms – must become the default mode of operation – in all countries and for all organizations.

And that can only happen if we understand that Privacy by Design is more than just a technological solution – it is among other things, a philosophy, a "culture of privacy."

By "culture of privacy," we mean a "mindset" – a way of thinking throughout an organization that is committed to better information management and the protection of privacy.



Organizations need to ensure that privacy is interwoven into the fabric of their day-to-day operations if privacy is to survive well into the future, because even the most advanced technology, coupled with the most rigorous privacy policies, will not be effective if they do not become an accepted part of organizational culture.

Privacy is part of the essential foundation upon which free and democratic societies are built.

The right to control the collection, use and disclosure of information about oneself is the right upon which other freedoms – freedom of association, freedom of movement, and the freedom to live as we choose – rest.

Therefore, to preserve privacy is to preserve that which is cherished but often taken for granted – the freedom and liberty that define the open society in which we live.

It is this understanding that has fuelled Dr. Cavoukian's longstanding interest in protecting the privacy rights of individuals, and that has so powerfully cemented her dedication to the cause and has led to Privacy by Design.

Over the years, we've seen many developments in the world of privacy. We've also seen the world change in ways that no one could have anticipated, even 20 years ago. And with these changes – the growing deployment of biometrics, Radio Frequency Identification, online social networks, and cloud computing, among many others – have come new challenges to privacy and our ability to exercise that right effectively.

But unlike some critics, who see technology as necessarily eroding privacy, Dr. Cavoukian has long taken the view that technology is inherently neutral. As much as it can be used to chip away at privacy, its support can also be enlisted to protect privacy through the use of Privacy-Enhancing Technologies (PETs) – a term she developed in 1995 when she co-authored a paper with Peter Hustinx of the Netherlands Data Protection Authority, where the argument was put forward that, yes, legal instruments are useful in protecting privacy, but they are not enough.

It was also back in the 1990s when Dr. Cavoukian first developed the concept of “Privacy by Design” – that we must enlist the support of technology to protect privacy and ensure that privacy is embedded into the design specifications to ensure its ongoing presence – even back then it was clear to her that the time was upon us when regulation and policy would no longer be sufficient to safeguard privacy.

At that time, this approach was considered to be quite controversial. Now, we are glad to say, it has gained broad acceptance – it was eventually understood that with the increasing complexity and connectivity of information technologies, nothing short of building privacy right into system design could suffice.

More recently, she has evolved the concept of PETs, extending it to “PETs Plus,” by adding one new component – a positive-sum paradigm.

The prevailing zero-sum model, wherein privacy is pitted against security, or against business practices, is destined to fail – heralding the demise of privacy.

However, if we change the paradigm to an inclusive positive-sum model, which allows the existence of privacy alongside functionality and performance, then the future of privacy grows more certain.

Up until now, Dr. Cavoukian's focus has also largely been on building privacy into information technologies.

Additionally, she has begun to work more closely with organizations, both public and private sector, to build privacy tools into accountable business practices and into physical design and infrastructure – from privacy breach protocols to the layout of hospital waiting rooms, opportunities abound to treat privacy as a design concept from the outset, and to achieve privacy objectives alongside other operational goals. This is called the Privacy by Design Trilogy.

We must cement the idea that privacy interests operate in a positive-sum model – meaning we must not trade off privacy against other goals like security or business profitability. It is indeed possible, desirable, and feasible to have it all, and we can do that with the careful application of the principles of Privacy by Design.

This past summer Dr. Cavoukian issued a new publication entitled, *Privacy by Design: The 7 Foundational Principles*, which clearly outlines the characteristics of *Privacy by Design* – the benefits of which ensure privacy and personal control over one’s information and, for organizations, gaining a sustainable competitive advantage.

In short, the seven principles are:

1. *Proactive* not *Reactive*; *Preventative* not *Remedial*
2. Privacy as the *Default*
3. Privacy *Embedded* into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

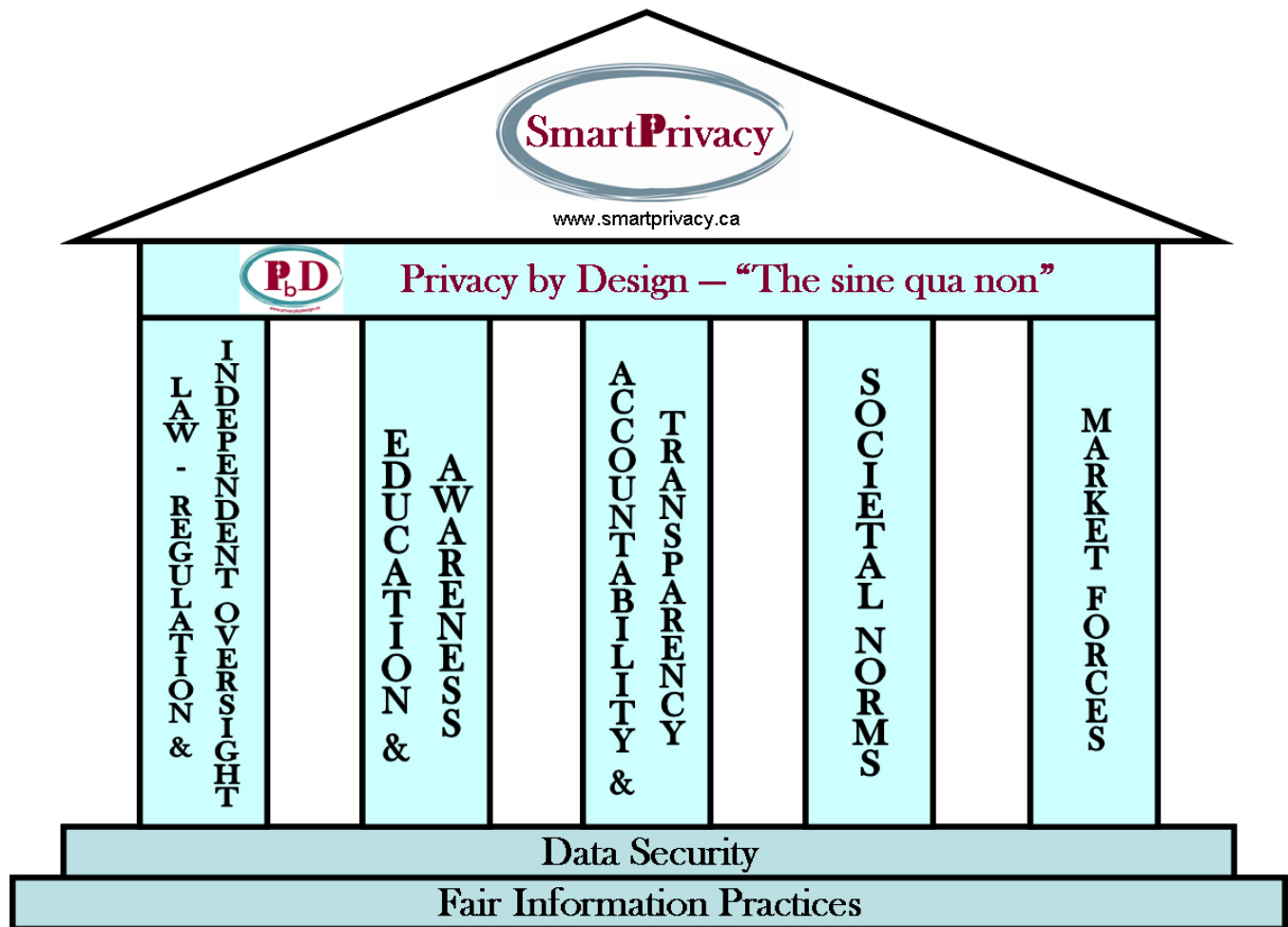
While her concept and vision of Privacy by Design has evolved over the years, what has remained constant throughout these evolutions is her firm conviction that a future without Privacy by Design – a future where privacy is not integrated thoughtfully and consistently into the very fabric, the very lifeblood of an organization – is a future in which privacy will cease to exist.

Further, recognizing that a multiplicity of forces act upon an organization’s ability to protect privacy, Dr. Cavoukian developed a model called SmartPrivacy to better describe the holistic approach necessary to realize the objective of Privacy by Design.

SmartPrivacy represents a tool-kit of protections, encapsulating everything necessary to ensure that all of the personal information in an organization is appropriately managed.

Each element of the model is important, but her concept of Privacy by Design represents its *sine qua non* because those who fail to envision privacy requirements early in the development of technologies, business practices and physical space will, despite the presence of the other elements, either fail to protect personal information or do so in a sub-optimal manner.

The SmartPrivacy model lends itself to a simple architectural metaphor.



“SmartPrivacy” is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: *Privacy by Design*. Dr. Ann Cavoukian, *Information & Privacy Commissioner of Ontario, Canada, August 13, 2009*.

Under the roof of SmartPrivacy which is supported by the joist of Privacy by Design stand five pillars.

1. Law, Regulation and Independent Oversight
2. Education and Awareness
3. Accountability and Transparency
4. Societal or Cultural Norms -
5. Market Forces

And these five pillars stand upon the foundations of Data Security and Fair Information Practices.



## 5. Conclusion

The IPC has been extremely active in building awareness of online privacy issues among young people, especially as they related to online social networks. Using a variety of channels and media, our focus has been on helping youth understand risks and empowering them to make conscious choices about when, how, and with whom they share personal information.

Youth, like other demographic groups, can benefit tremendously from the Internet and all it has to offer. But they must do so with their eyes wide open, using their judgement to stay in control of their personal information and, ultimately, of their reputations.

The IPC looks forward to further opportunities to help make young people more privacy-savvy when they engage in online activities, and to encourage key stakeholders to make more privacy-enhancing options available online.



Published: October 2009

**Information and Privacy Commissioner,  
Ontario, Canada**

2 Bloor Street East, Suite 1400  
Toronto, Ontario • M4W 1A8 • Canada

Telephone: 416-326-3333 • 1-800-387-0073

Facsimile: 416-325-9195

TTY (Teletypewriter): 416-325-7539

Email: [info@ipc.on.ca](mailto:info@ipc.on.ca)

Website: [www.ipc.on.ca](http://www.ipc.on.ca)

Privacy by Design: [www.privacybydesign.ca](http://www.privacybydesign.ca)