New Ways of Dealing with Privacy:
Think Positive-Sum, Not Zero-Sum

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario

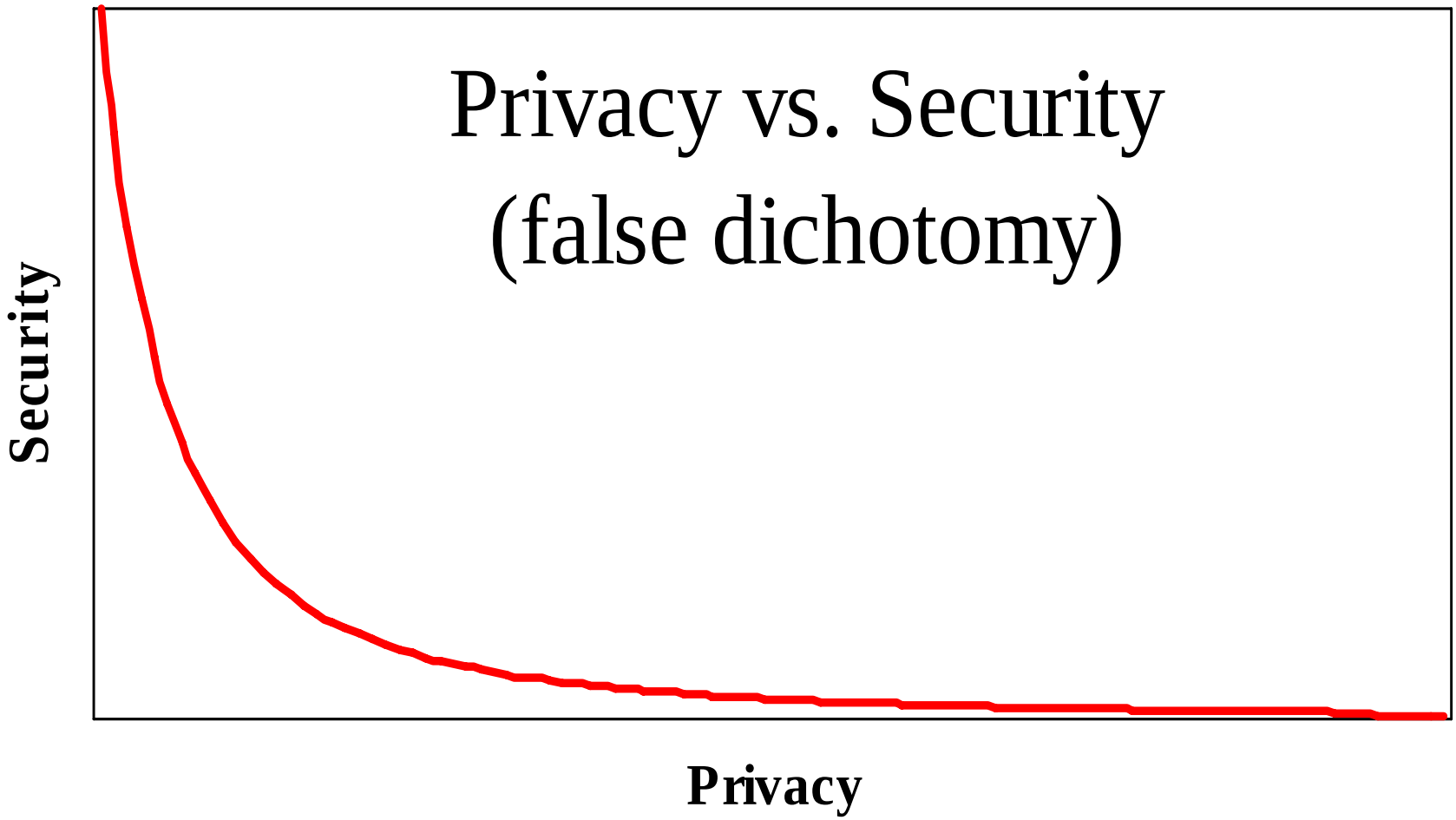
International Association of Privacy Professionals
Canadian Privacy Summit 2008
Toronto, Canada
May 22, 2008

Presentation Outline

1. *Looking at Privacy Differently*
2. *Transformative Technologies*
3. *Video Surveillance Transformed*
4. *RFID (Radio Frequency Identification)*
5. *Transformative Business Practices*
6. *Online Social Networking*
7. *Conclusions*

Looking at Privacy Differently

Privacy OR Security:
A Zero-Sum Game



Positive-Sum Model

Change the paradigm
from a zero-sum to
a positive-sum model:
Create a "win-win" scenario,
not an "either/or"
involving trade-offs

Looking at Privacy Differently

Old World: Zero-sum mentality

Future: Positive-sum paradigm

Don't get stuck in the past

Transformative Technologies

Transformative Technologies

Surveillance Technology + Positive-Sum Paradigm = Transformative Technologies

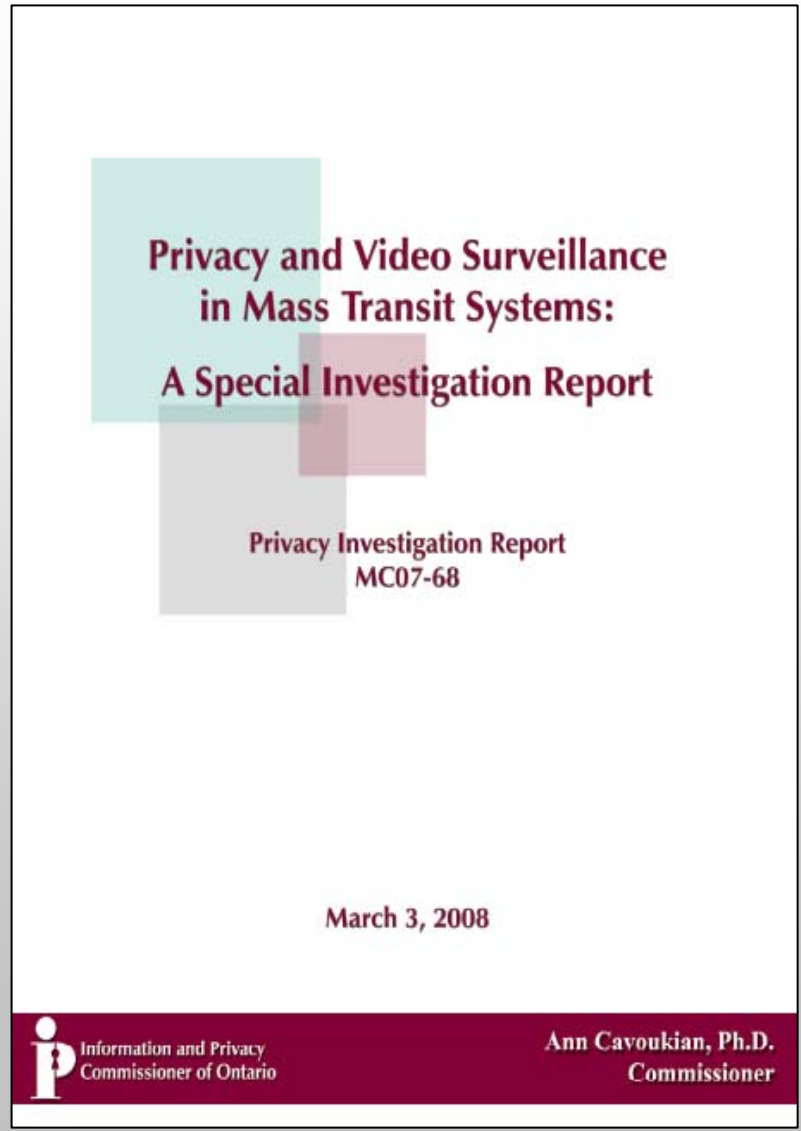
Common characteristics of Transformative Technologies:

- Minimize unnecessary disclosure, collection, retention and use of personal data;
- Empower individuals to participate in the management of their own personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in personal data governance structures;
- Promote and facilitate widespread adoption of privacy-protective technologies and business practices.

Video Surveillance Transformed

TTC Surveillance Cameras

- In March 2008, I ruled that the Toronto Transit System's expansion of its video surveillance system, for the purposes of public safety, was in compliance with Ontario's *Municipal Freedom of Information and Protection of Privacy Act.*
- However, I called upon the TTC to undertake a number of specific measures to enhance privacy.
  - Personal information will only be collected for legitimate, limited and specific purposes;
  - Collection will be limited to the minimum necessary and only retained up to 72 hours;
  - Personal information will only be used and disclosed for the specified purposes.



www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

Innovative Privacy-Enhancing Approach to Video Surveillance

- At the University of Toronto, Karl Martin and Prof. Kostas Plataniotis, have developed a privacy-enhancing approach to video surveillance;
- Their work uses cryptographic techniques to secure a private object so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key;

(a) (b) (c)

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

- Objects of interest (face or body) are stored as completely separate entities from the background surveillance frame, and efficiently encrypted.

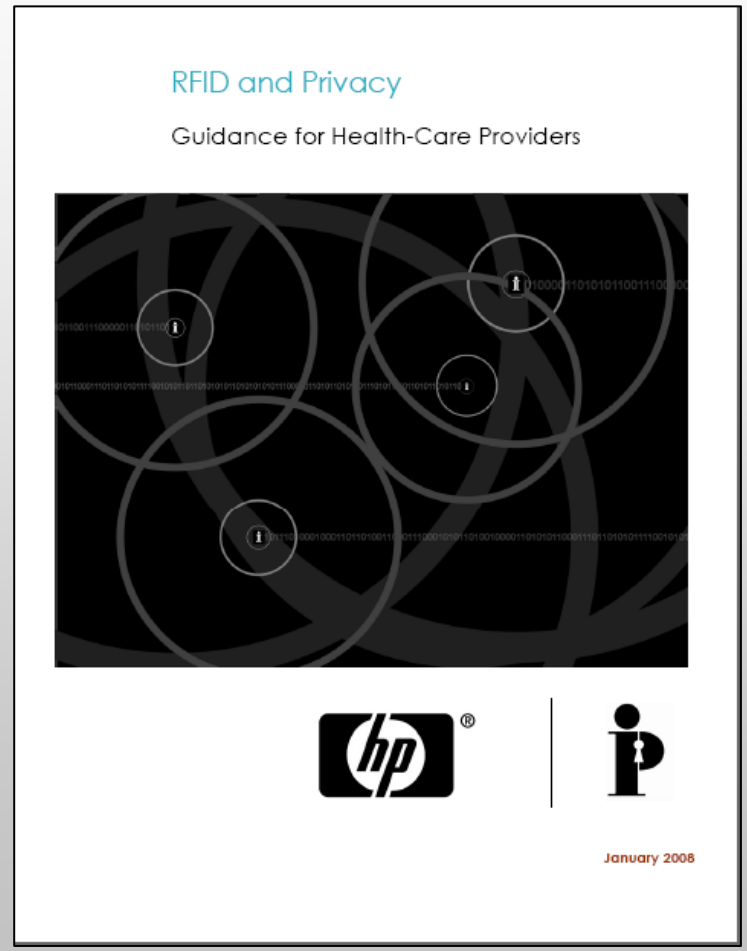
RFID

Radio Frequency Identification

RFID and Privacy in Health Care:
Guidance for Health Care Providers

- This paper is organized into three broad categories according to the increasing level of potential risk to privacy:

1. RFID technology to track things;
2. RFID technology to track things associated with people; and
3. RFID technology to track people.



www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf

RFID Transformed

Approaches to ensuring end-user privacy:

1. **RFID Kill Function**: RFID tags can be deactivated;
2. **Physical Privacy**: Reading of RFID tags is physically restricted (e.g. IBM clipped tag): effectively "killed" but allows for reactivation;
3. **On-Tag Scheme**: Readers communicate directly with tags that can control access to their content;
4. **Agent Scheme**: Users delegate privacy management to a privacy agent;
5. **User Scheme**: Users authorize each individual read-out process themselves.

Transformative Business Practices

Permission-Based Marketing: The Personal Touch

- Essential premise: persuade consumers to ***volunteer*** their attention;
- Predicated on consent: makes consumers *active* recipients of marketing information;
- Puts control in the hands of consumers.

— Seth Godin,
Permission-Based Marketing, 2001.

Relating to Customers – 1:1

"The 1:1 enterprise, operating in an interactive environment, relies not just on information *about* customers, but information *from* them."

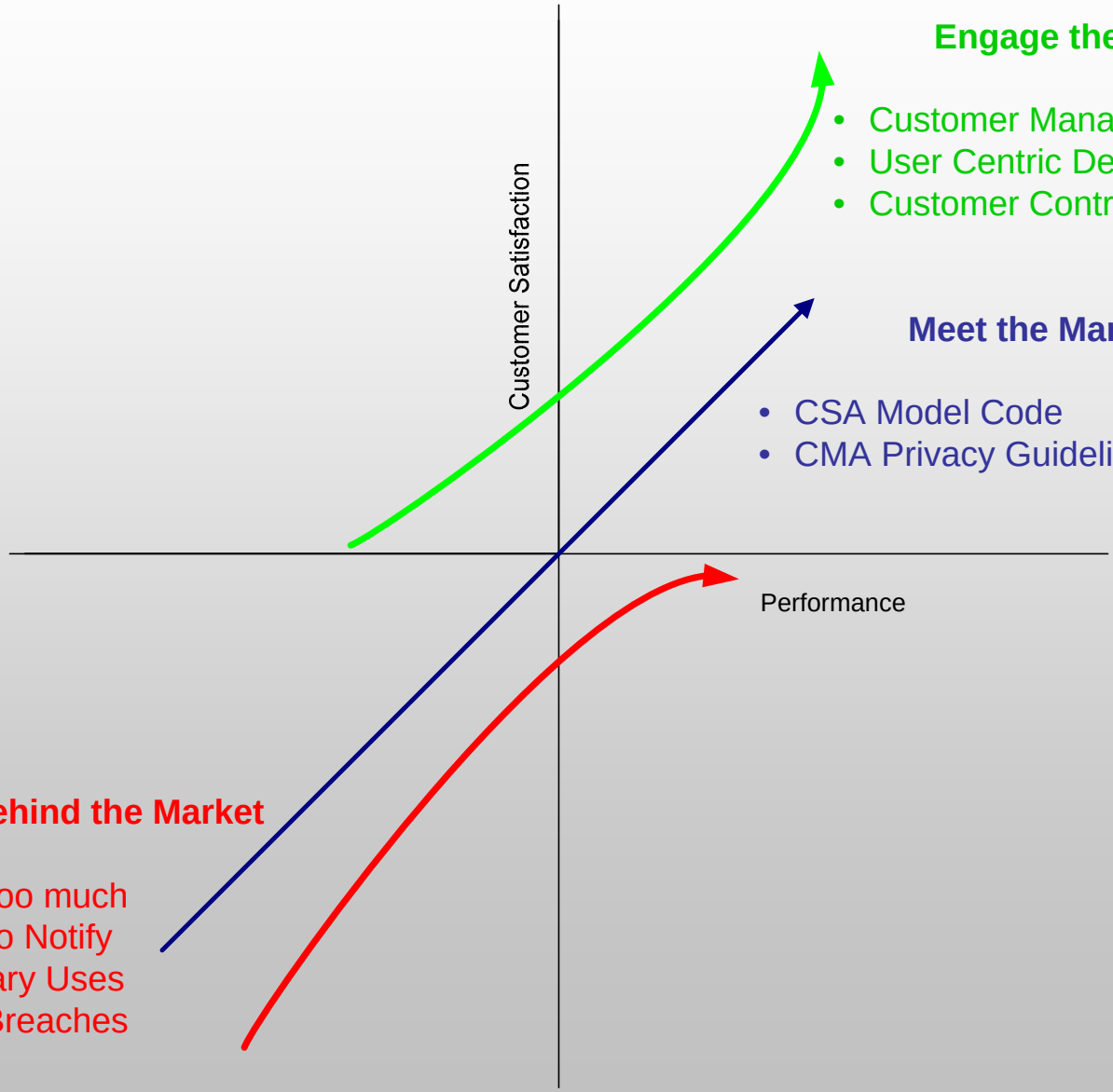
"It is absolutely imperative for the 1:1 enterprise to take into account the issue of protecting individual customer privacy."

– Don Peppers and Martha Rogers, Ph.D.,
Enterprise One to One: Tools for Competing in the Interactive Age, 1996.

The CMR Challenge

- Become more customer-centric: Change from CRM (Customer Relationship Management) to **CMR: Customer Managed Relationships**;
- **NOT:** "Know everything about your customers." **Replace with:** "Know everything that your customers ***want*** you to know, and are willing to give you;"
- Lead by assuming nothing, instead, ***always ask*** – think of this as a simple yet highly effective customer retention strategy.

Privacy and the Market



Engage the Customer

- Customer Managed Relationships
- User Centric Design
- Customer Control of Data

Meet the Market

- CSA Model Code
- CMA Privacy Guidelines

Behind the Market

- Collect too much
- Failure to Notify
- Secondary Uses
- Visible Breaches

Online Social Networking

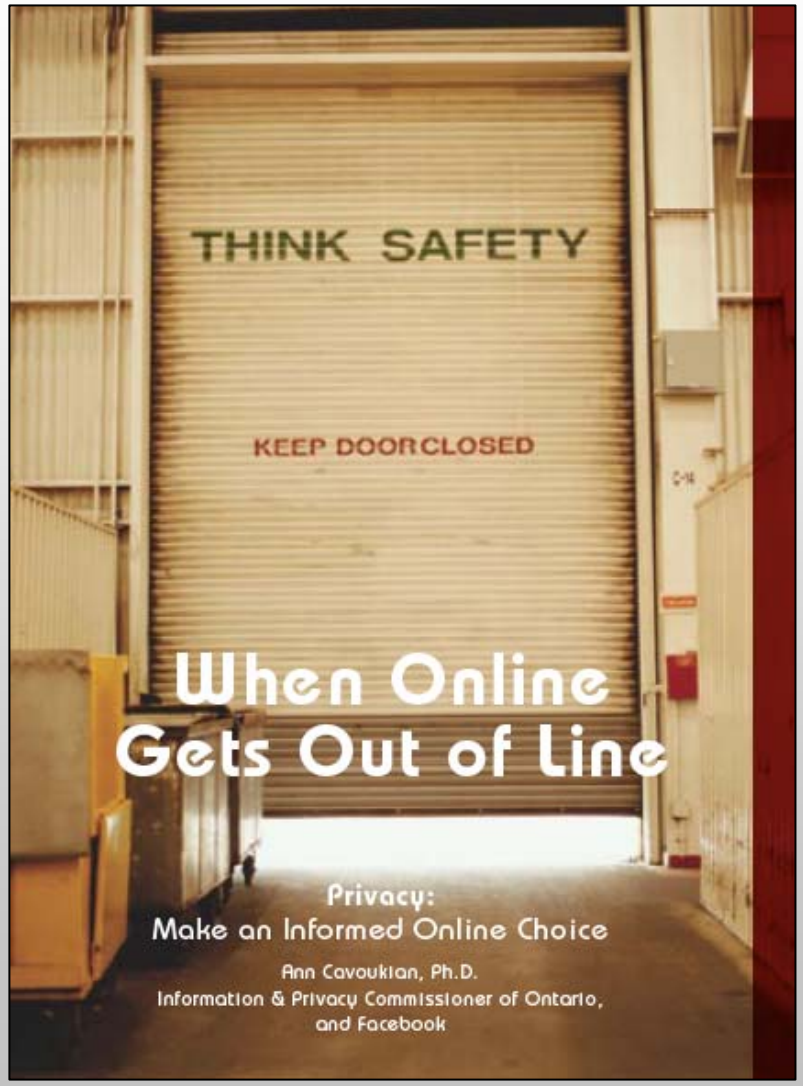
Online Social Networks

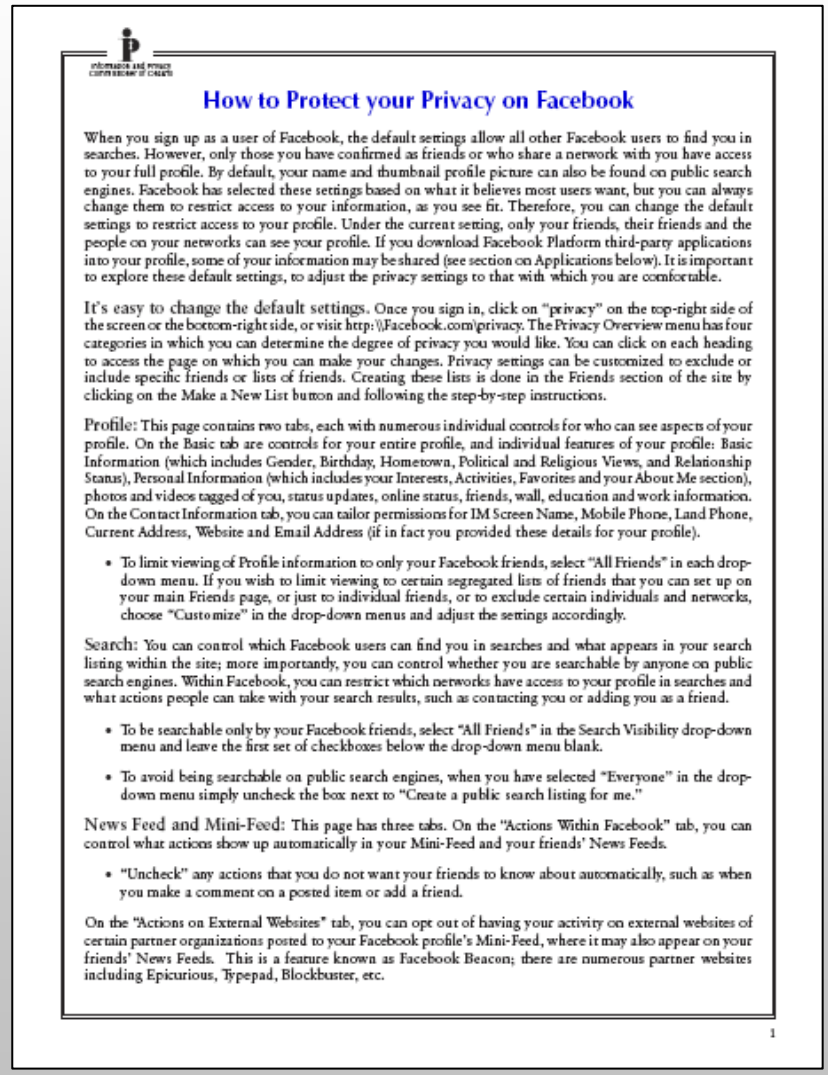
- Online social networks are about data disclosure, not data minimization, so where does privacy fit in?
- Privacy practices and controls play an important role if they're factored directly into the design;
- Online social networks can allow users to tightly limit disclosure – even at very granular levels;
- Users can place strong privacy controls on the dissemination of their information on Facebook, if they choose to.

Protecting Your Privacy on Facebook
IPC Video

- Two years ago, I was approached by Facebook for my input on their privacy measures;
- My office developed several brochures and a detailed Tip Sheet for the public: *How to Protect Your Privacy on Facebook*;
  — www.ipc.on.ca/images/Resources/facebk-protectpriv_442945156250.pdf
- Today, we are announcing the release of a new video offering guidance on how to protect your privacy on Facebook: *Be a Player: Take Control of Your Privacy on Facebook.*

IPC Facebook Publications





How to Protect your Privacy on Facebook

When you sign up as a user of Facebook, the default settings allow all other Facebook users to find you in searches. However, only those you have confirmed as friends or who share a network with you have access to your full profile. By default, your name and thumbnail profile picture can also be found on public search engines. Facebook has selected these settings based on what it believes most users want, but you can always change them to restrict access to your information, as you see fit. Therefore, you can change the default settings to restrict access to your profile. Under the current setting, only your friends, their friends and the people on your networks can see your profile. If you download Facebook Platform third-party applications into your profile, some of your information may be shared (see section on Applications below). It is important to explore these default settings, to adjust the privacy settings to that with which you are comfortable.

It's easy to change the default settings. Once you sign in, click on "privacy" on the top-right side of the screen or the bottom-right side, or visit http://Facebook.com/privacy. The Privacy Overview menu has four categories in which you can determine the degree of privacy you would like. You can click on each heading to access the page on which you can make your changes. Privacy settings can be customized to exclude or include specific friends or lists of friends. Creating these lists is done in the Friends section of the site by clicking on the Make a New List button and following the step-by-step instructions.

Profile: This page contains two tabs, each with numerous individual controls for who can see aspects of your profile. On the Basic tab are controls for your entire profile, and individual features of your profile: Basic Information (which includes Gender, Birthday, Hometown, Political and Religious Views, and Relationship Status), Personal Information (which includes your Interests, Activities, Favorites and your About Me section), photos and videos tagged of you, status updates, online status, friends, wall, education and work information. On the Contact Information tab, you can tailor permissions for IM Screen Name, Mobile Phone, Land Phone, Current Address, Website and Email Address (if in fact you provided these details for your profile).

- To limit viewing of Profile information to only your Facebook friends, select "All Friends" in each drop-down menu. If you wish to limit viewing to certain segregated lists of friends that you can set up on your main Friends page, or just to individual friends, or to exclude certain individuals and networks, choose "Customize" in the drop-down menus and adjust the settings accordingly.

Search: You can control which Facebook users can find you in searches and what appears in your search listing within the site; more importantly, you can control whether you are searchable by anyone on public search engines. Within Facebook, you can restrict which networks have access to your profile in searches and what actions people can take with your search results, such as contacting you or adding you as a friend.

- To be searchable only by your Facebook friends, select "All Friends" in the Search Visibility drop-down menu and leave the first set of checkboxes below the drop-down menu blank.
- To avoid being searchable on public search engines, when you have selected "Everyone" in the drop-down menu simply uncheck the box next to "Create a public search listing for me."

News Feed and Mini-Feed: This page has three tabs. On the "Actions Within Facebook" tab, you can control what actions show up automatically in your Mini-Feed and your friends' News Feeds.

- "Uncheck" any actions that you do not want your friends to know about automatically, such as when you make a comment on a posted item or add a friend.

On the "Actions on External Websites" tab, you can opt out of having your activity on external websites of certain partner organizations posted to your Facebook profile's Mini-Feed, where it may also appear on your friends' News Feeds. This is a feature known as Facebook Beacon; there are numerous partner websites including Epicurious, Typepad, Blockbuster, etc.

1

Available at: www.ipc.on.ca

Conclusions

- It is highly unlikely that surveillance technologies such as video cameras, are going to be entirely eliminated – however, they *can* be transformed;
- **Transformative technologies** maintain the functionality of such technologies and yet transform them to operate in a privacy-protective manner;
- We can no longer sustain the **"privacy vs. functionality/ privacy vs. security"** mentality;
- Adopting a positive-sum paradigm of **"privacy AND functionality/security"** where privacy is built right into the design, is a far more efficient and productive approach, leading to a "win/win" for all sides.

How to Contact Us

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca