

Information Security  
It's *Your* Responsibility



Manitoba 

# Introduction

## Privacy and Security

- Are they the same thing
- How are they similar
- Can one exist without the other
- Why are they confused
- How can they collide
- How we must work together

## Definitions

- ***Personal Information (PI)***: Information about an identifiable individual
- ***Privacy***: Control over one's own PI
- ***Confidentiality***: Control over another's PI or confidential information
- ***Security***: The ability to implement privacy or confidentiality

## **Examples of Private Information**

Recorded information about an individual:

- Name
- Home address
- Age, sex, sexual orientation
- Race, nationality
- Identifying numbers (SIN)

## **Examples of Security**

- Policy, Standards, Guidelines
- Risk Assessment & Management
- Firewalls
- Encryption
- Forensics
- Monitoring technologies
- Physical security
- Other technology (Anti Virus, Spyware)

# Privacy

Name

Address

Sex, sexual orientation

Identifying Numbers

Race, Nationality

≠

≠

≠

≠

≠

# Security

Policy

Risk Management

Forensics

Monitoring

Other Security Technologies

*In fact some privacy advocates have concerns with a number of security related technologies*

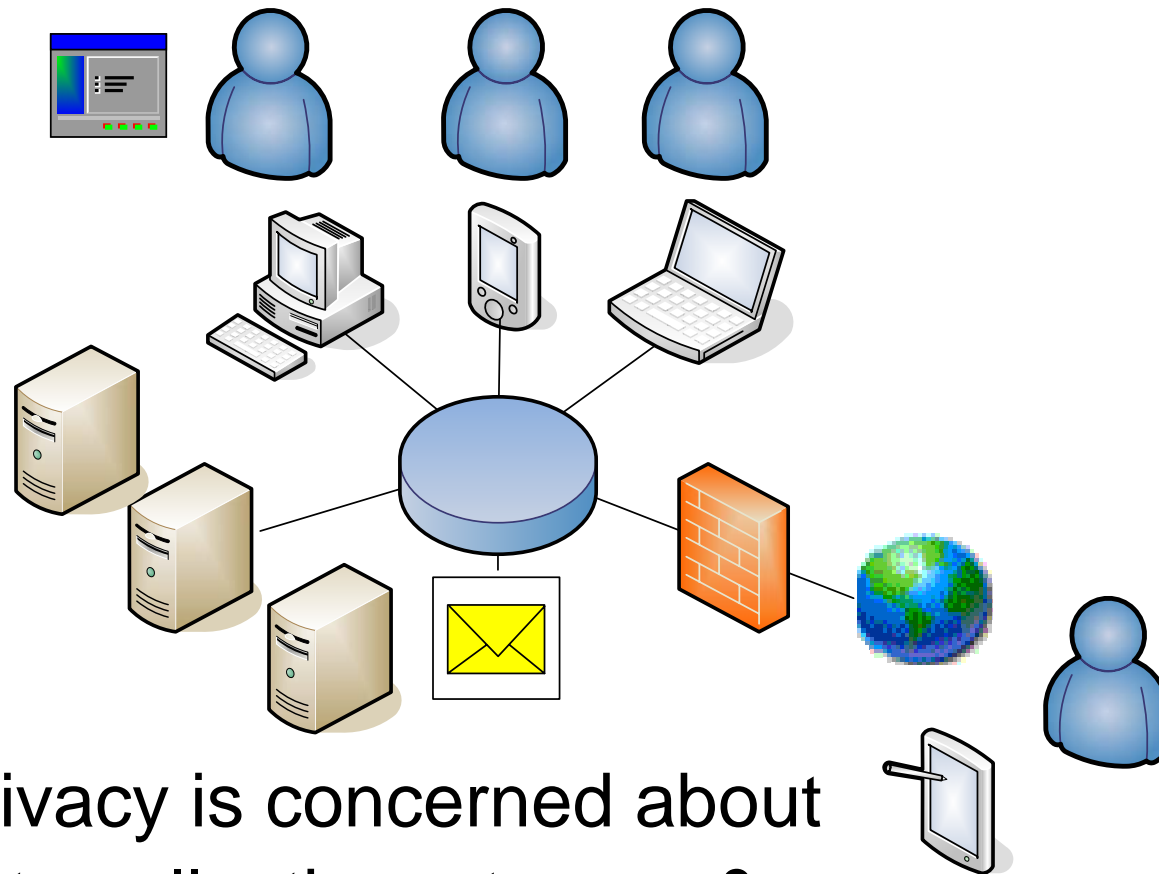
## **Collisions**

Privacy and security can have conflicting views:

- Example US Patriot Act
- Claims to enhance the security of Americans
  - Increased surveillance powers
- Privacy advocates have significant concerns with the Patriot Act in the USA
  - Clauses affect Canadian outsourcing

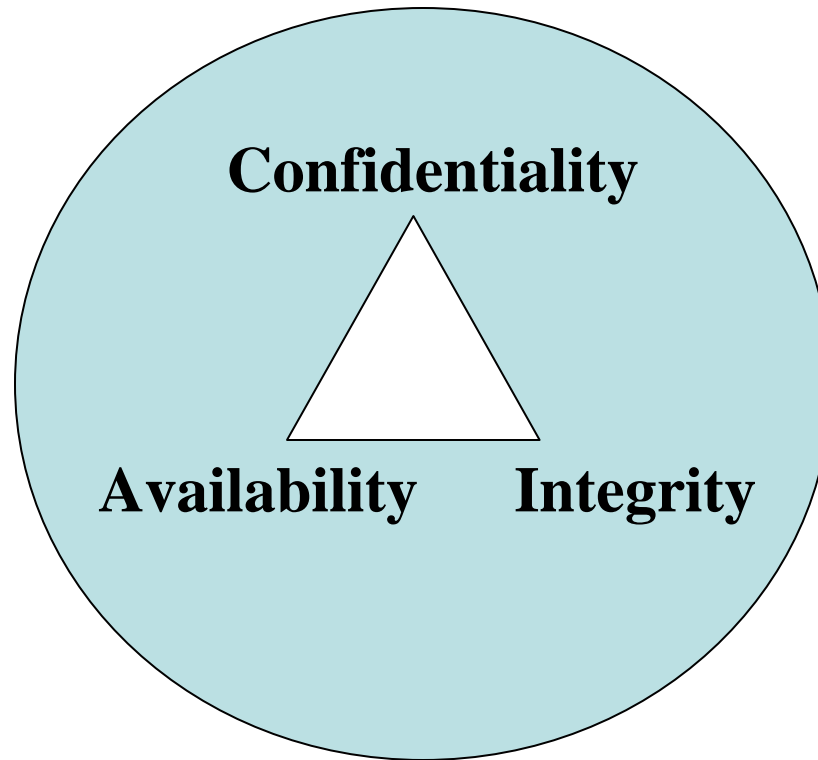
# Information Security

Security touches every aspect of an organization



Privacy is concerned about data collection, storage & use

## Triad of Security (CIA)



*Privacy is most often concerned with Confidentiality and Integrity of data*

## Privacy and Security

*Although privacy and security goals may at times seem at odds, successful organizations ensure that privacy and security initiatives are clearly explained, well understood, and complementary.*

# Complementary Roles

PRIVACY – Collection, use & disclosure limits, access, openness, etc.

PRIVACY + SECURITY – access control, trust management, authentication, authorization, etc.

SECURITY – encryption, control over malicious attacks, security architecture, etc.



## Privacy Protection starts with a PIA

- Identify the information you will collect
- Collect only the minimum that is needed
- Make sure you have a legal right to collect
- Protect what you collect

*As business owners make sure you know what your IT systems collect!*

## **Complementary Processes**

- Privacy Impact Assessments
  - Identifies personal information
- Business Impact Assessments
  - Identifies the impact on the business
- Risk assessments
  - Selection of the security controls

## Reality Check

- Security  $\neq$  Privacy
- Possibilities:
  - Perfect security, perfect privacy
  - No security, no privacy
  - Perfect security, no privacy
- Impossibility:
  - No security, perfect privacy

*Security is a prerequisite for privacy, but it is not the same thing as privacy.*

## Where does the confusion come from?

We've already said that:

- You can have secure systems that don't respect privacy
- You can have insecure systems respect privacy principles

*Security is often the last line of defence for addressing privacy issues not addressed during the design phase*

## Example

Application developed for the Internet

- Limited collection of personal information
- Yet developers chose to use the SIN number as a unique ID within the system
  - No longer collecting what was needed
- Security steps in and demands changes
  - Security blamed for delay in going live
- Root cause - failure to address privacy

## **The Answer – Risk Assessment**

- Business units must assess risk
- Take into account privacy concerns
- Put in place optimal security through a risk assessment
  - The right amount of security

## What does FIPPA say about Security?

*The head of a public body shall protect personal information by making reasonable arrangements against such risks as unauthorized access, use, disclosure, or destruction.*

## Respect Privacy

We must respect privacy, it's the law!

- Citizens expect and demand it
- 58% of consumers say they will terminate their relationship with an organization who compromises their data
- One third said they would take legal action

*(Source EDS Privacy Survey)*

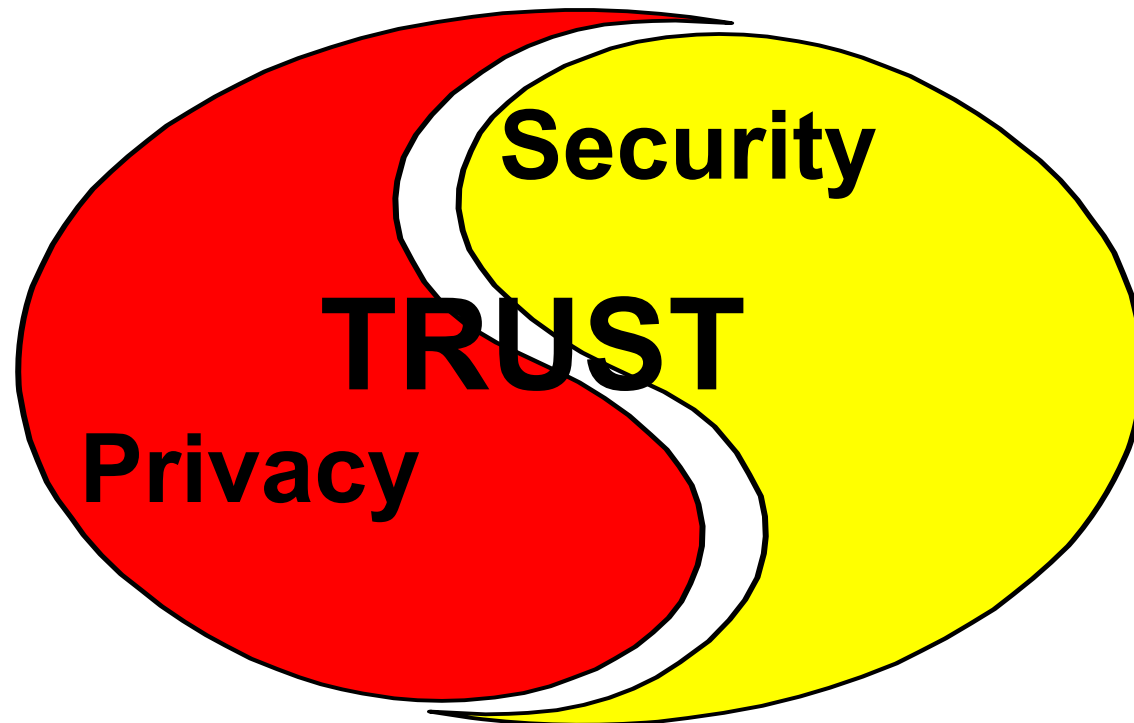
## **Service Transformation**

- Every government has some form of service transformation initiative under way
- Reduce costs by self service through web
- 69% of business owners say that breaches in data security will negatively impact their organization
- Citizens who don't trust the Government will not do business online

## **Conclusions**

- We must respect privacy
- A PIA is part of the solution
- We have a legal obligation to protect data
- We must work together, Privacy & Security
- We must add value to the business
- We must enable service delivery

Privacy + Security =  
Privacy + Security + Trust



# Questions?

Patrick Hoger

CISO

Manitoba Government

Information Protection Centre

