BLISS informatics

How Badly Broken is Privacy Legislation?

And what can we do to fix it?

17th Annual Privacy and Security Conference
Privacy and Security by Choice, not Chance
Afternoon Workshop
Wednesday February 3, 2016
Victoria, B.C. Canada

Gerry Bliss gbliss@shaw.ca 250-881-6179

Agenda

- Welcome and Introduction
- Privacy and ethics
- History of privacy in law
- What were they thinking?
- How far are we from where should be?
- Why are we getting it wrong?
- Can we get it right?
- What's the fix?

Goal

- Provide you with additional context for understanding and interpreting privacy legislation
- Trigger discussion and debate
- Encourage advocacy and engagement in the lawmaking process.
- Add to your enthusiasm and optimism as privacy practitioners and advocates.

Rules of Engagement

- 3 hours – 2 breaks on the hour
- Safe environment
  - Frank and honest discussion
  - Respectful collegial disagreement
- Ask
  - If I need to clarify
  - If I've set your hair on fire

We are all in this together…

Gerry's Bio

- 30+ years as an informatician
  - Data warehouse and applied analytics
  - IT development, operations and corporate client service
- 20+ years as an information risk manager
  - CSO, CPO, consultant, advocate, teacher
  - SCORM based web base training tool development
- 5 years in formal academic role
  - Ethics, legal issues, and cybersecurity
  - Research privacy

Gerry Bliss gbliss@shaw.ca 250-881-6179

A Quick Poll...

- Who thinks privacy and access legislation is working the way it should?
- Who thinks privacy and access legislation is broken and can be fixed?
- Who thinks privacy and access legislation is beyond repair?

Working Definitions

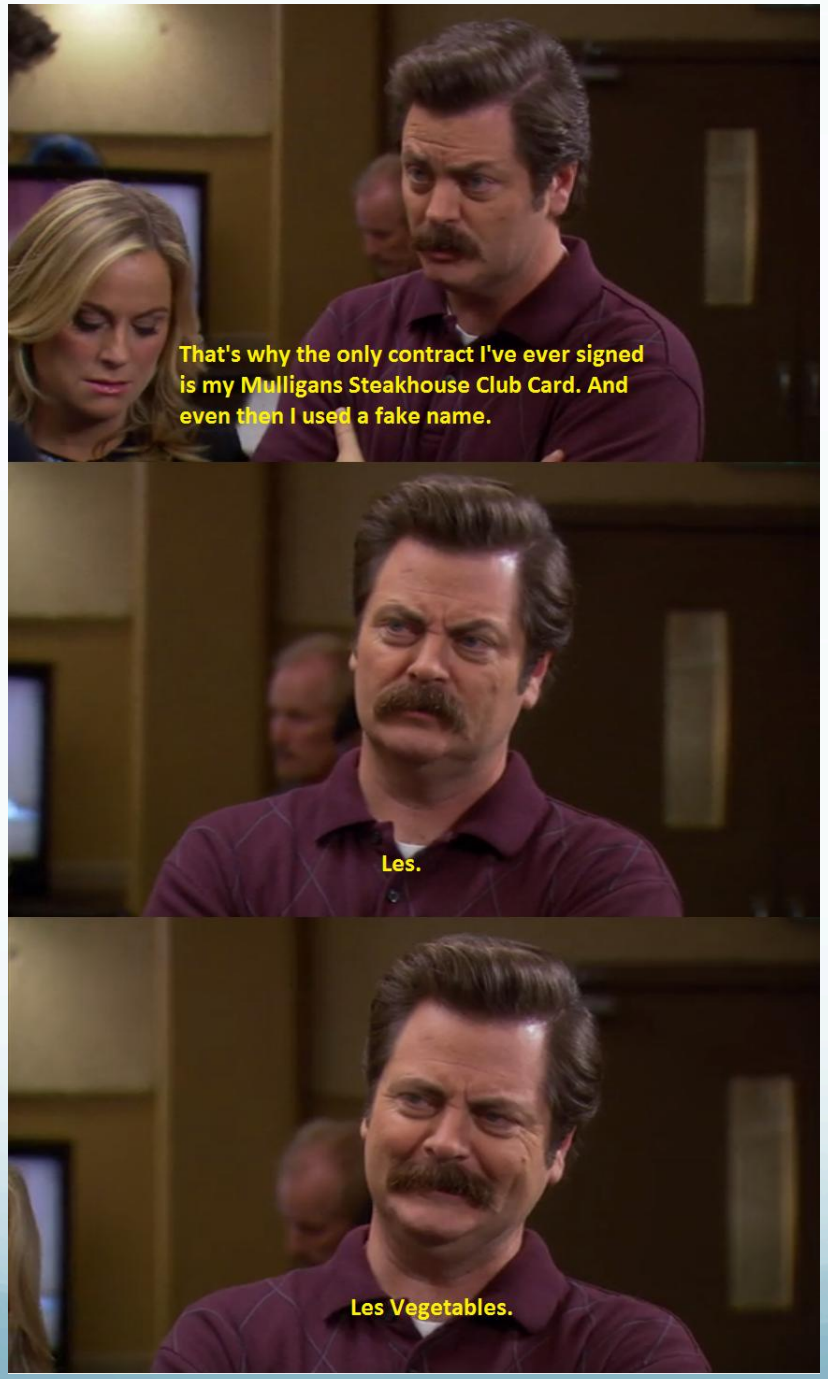
Privacy: one's right to control who has access to information about oneself

Confidentiality: a duty owed by one to preserve the personal information of another

Security: controls put in place to safeguard privacy and ensure confidentiality is maintained

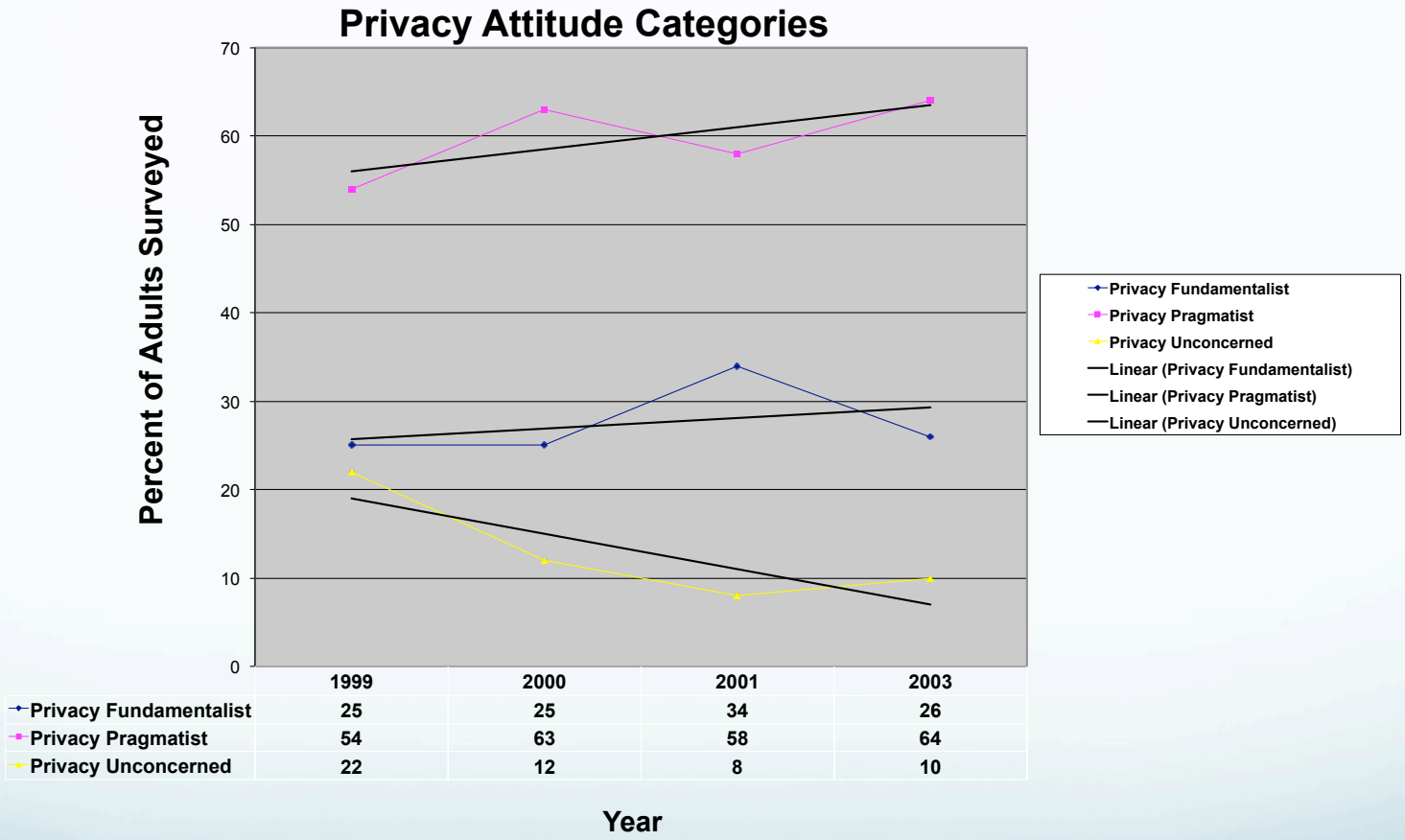
Access: 1. the ability to view and update one's own information as required. **2.** reasonable access to government information that does not meet specific access exclusion criteria.

Some people are more protective of their privacy than others...



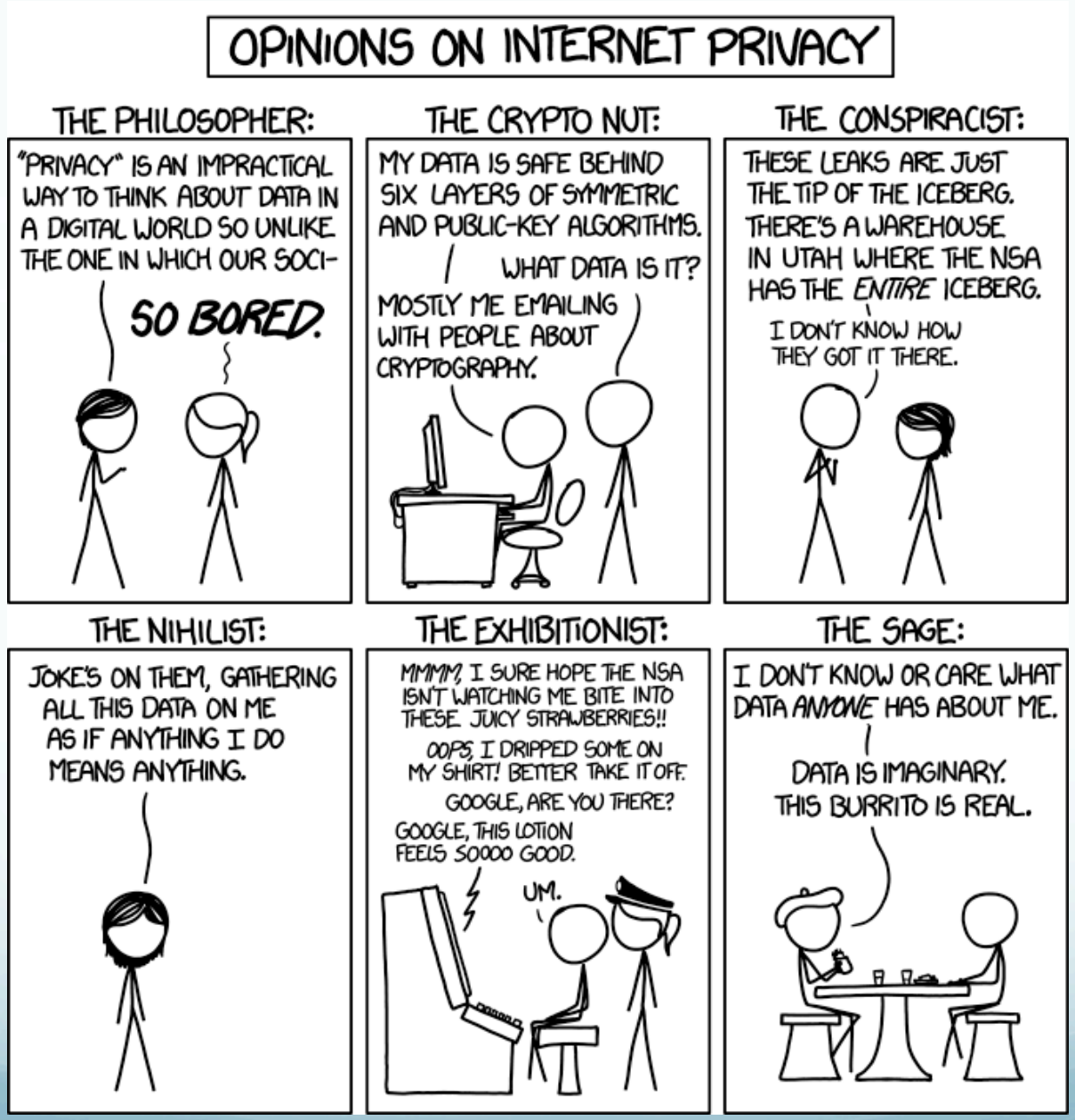
Eg. Ronald Ulysses Swanson

Privacy Attitudes



	1999	2000	2001	2003
Privacy Fundamentalist	25	25	34	26
Privacy Pragmatist	54	63	58	64
Privacy Unconcerned	22	12	8	10

(Source: The Harris Poll #17. March 17th, 2003. Based on the research of Dr. Alan Westin, President and publisher of Privacy and American Business)



Ref. https://xkcd.com/1269/

Ethical Principles

1. Autonomy and Respect for Persons
2. Equality and Justice
3. Fidelity, Integrity, or Best Action
4. Principle of Beneficence
5. Principle of Non-Malfeasance
6. Principle of Impossibility

Autonomy and Respect for Persons

- Always treat persons as ends-in-themselves, not as objects or means to an end.
- Always treat persons as autonomous decision-makers.

Equality and Justice

- All persons are equal and should be treated the same.
- Exceptions to this must always be based on ethically relevant differences in the nature or status of the person in question.

Fidelity, Integrity, or Best Action

- Whoever has an obligation, has a duty to fulfill that obligation to the best of her or his ability.

Principle of Beneficence

- Everyone has a duty to advance the good of others:
  1. If it is possible to do so without undue risk to oneself.
  2. Where the nature of the good is in keeping with the competent values of the recipients of the action in question.

Principle of Non-Malfeasance

- Everyone has a duty to prevent harm:
  1. Insofar as this is possible without undue risk to oneself.
  2. Where the nature of the harm is in keeping with the competent values of the recipient of the action in question.

Principle of Impossibility

- No-one can have an obligation to do what it is impossible to do under the circumstances that apply
- Except when the impossibility is the result of inappropriate action by the individual who otherwise would have the relevant duty


HOW HARD WOULD IT BE TO PROGRAM OUR WEBSITE TO COLLECT BROWSER HISTORY FROM OUR VISITORS?
WELL, FIRST I'D NEED TO INVENT SOME SORT OF DEVICE THAT REVERSES MY SENSE OF RIGHT AND WRONG.
SO. . . ARE WE TALKING ABOUT A WEEK. . . OR A MONTH?
Dilbert.com DilbertCartoonist@gmail.com
©2011 Scott Adams, Inc./Dist. by UFS, Inc.

Ethical Principles Reflected in Legislation: **Privacy**

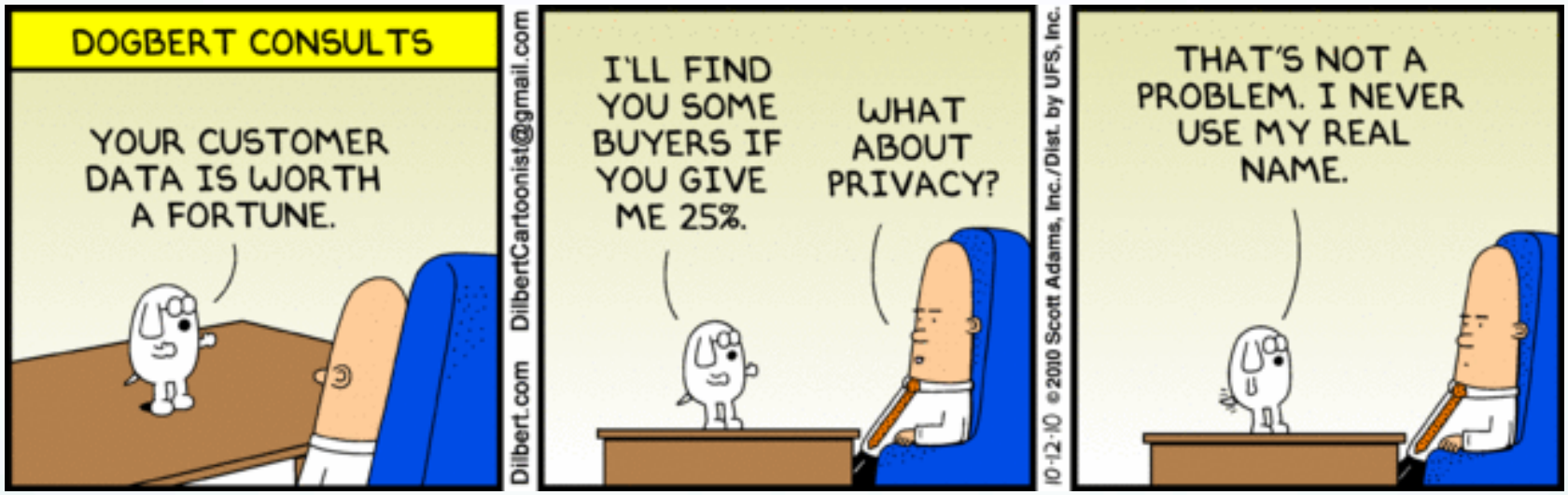
1. As an autonomous person, your information is yours to control – you can share it and unshare it.
2. You share your information with specified individuals for specific purposes by consent only. By default your consent state is set to "No"...
3. The custodian of your information is accountable for taking reasonable steps to:
    1. Control access and destruction
    2. Maintain accuracy
    3. Give you access

Ethical Principles Reflected in Legislation: **Access**

1. Access to information collected or created by the state is a right of citizenship and made available as a part of normal operation
2. If state information is not specifically exempted from access, it is reasonably accessible
3. Exemptions are based on reasonable assessment of harm to the state and citizens
4. The state custodian has an obligation to assist the citizen in accessing information

Privacy and Access Responsibilities

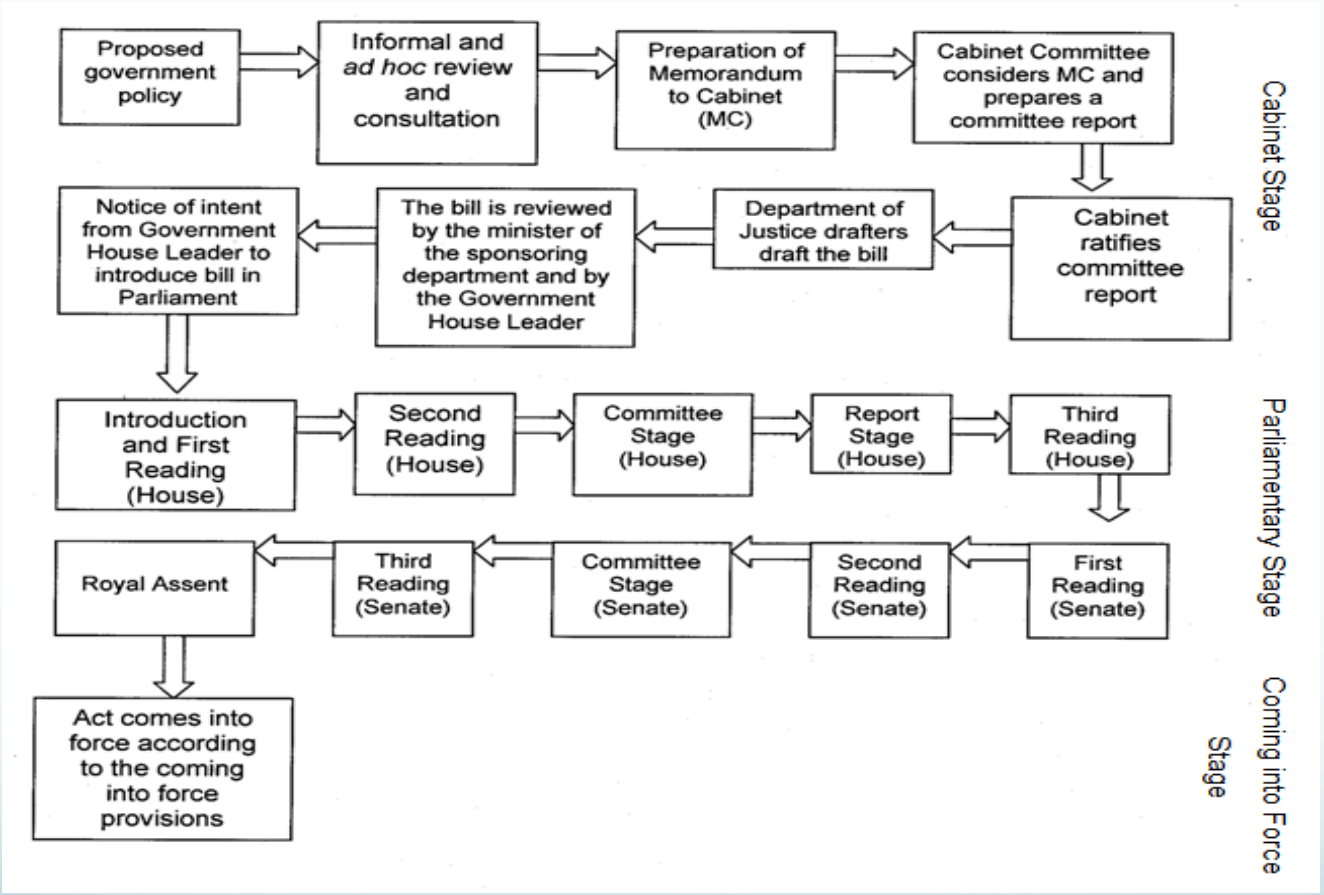
- Organization – protects personal information in it's custody and in transit through policy, process, and technical controls. Enables authorized access to individual and business information.
- Executive – set policy and example
- Management – ensure staff are aware of policy and procedure and are trained
- Staff – understand and meet privacy accountabilities. Assist clients with access.
- All – observe and report threats to privacy and access or weaknesses in controls


DOGBERT CONSULTS
YOUR CUSTOMER DATA IS WORTH A FORTUNE.
Dilbert.com DilbertCartoonist@gmail.com
I'LL FIND YOU SOME BUYERS IF YOU GIVE ME 25%.
WHAT ABOUT PRIVACY?
10-12-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.
THAT'S NOT A PROBLEM. I NEVER USE MY REAL NAME.

How Are Laws Made?

- "All laws begin with dreams." *George Elliot Clarke, Canadian Parliamentary Poet Laureate.*
- Some laws begin with nightmares...
- In Canada, law creation federally and provincially begin with legislators and a policy agenda, and ends with Royal assent.
- Most laws have foundations in ethical principles.
- Criminal, Contract, Tort

Federal Lawmaking Process Flow



Ref. http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0864-e.htm

Charter of Rights and Freedoms

- Section 7:
  - Right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.
  - Information cannot be achieved through state trickery and silence cannot be used to make inference of guilt.
- Section 8:
  - Right to be secure against unreasonable search or seizure.
  - Your home and your car are protected – your garbage is not.

A Brief History of Information and Privacy Law

- Documented privacy rights as far back as the Greeks - Hippocrates
- Personal rights and freedoms encoded over the past 2,000 years - Magna Carta (1215)
- Privacy and Access post WWII and the Holocaust: UN -1948 Universal Declaration of Human Rights, Article 12
- Canadian Constitution -1982 Charter Sec. 7 and 8
- Privacy Legislation: US -1974, Canada -1983, BC Privacy -1986, FIPPA -1996, PIPA - 2004
- Constitutional and case law – McInerney vs. MacDonald – Access (1992), R. v. Spencer – Privacy (2014)

What Were They Thinking?

- The proactive disclosure and access practices of the time would continue
- 30 day access was intended for information not normally disclosed
- Personal information was excluded from the 30 day access allowance
- The problem was smaller than it actually is
- The problem was less complex than it actually is
- Technology impact was underestimated
- Sometimes you have to pick what works over what's ideal

Political/Legal Changes

- 9/11, Al-Qaeda, ISIS, N. Korea driving new state security legislation worldwide
- State authorized hacking; organized crime based hacking
- State Surveillance: CSE, 2 million monitors for Chinese Internet, Increased domestic law enforcement surveillance
- Bills C-13 Passed October 2014; Bill C-51 August 2015
- Privacy tort precedents – non-compliance, theft, harm, breach of contract, invasion of privacy....
- Affirmation of rights to access and privacy in case and constitutional law

Technology Changes

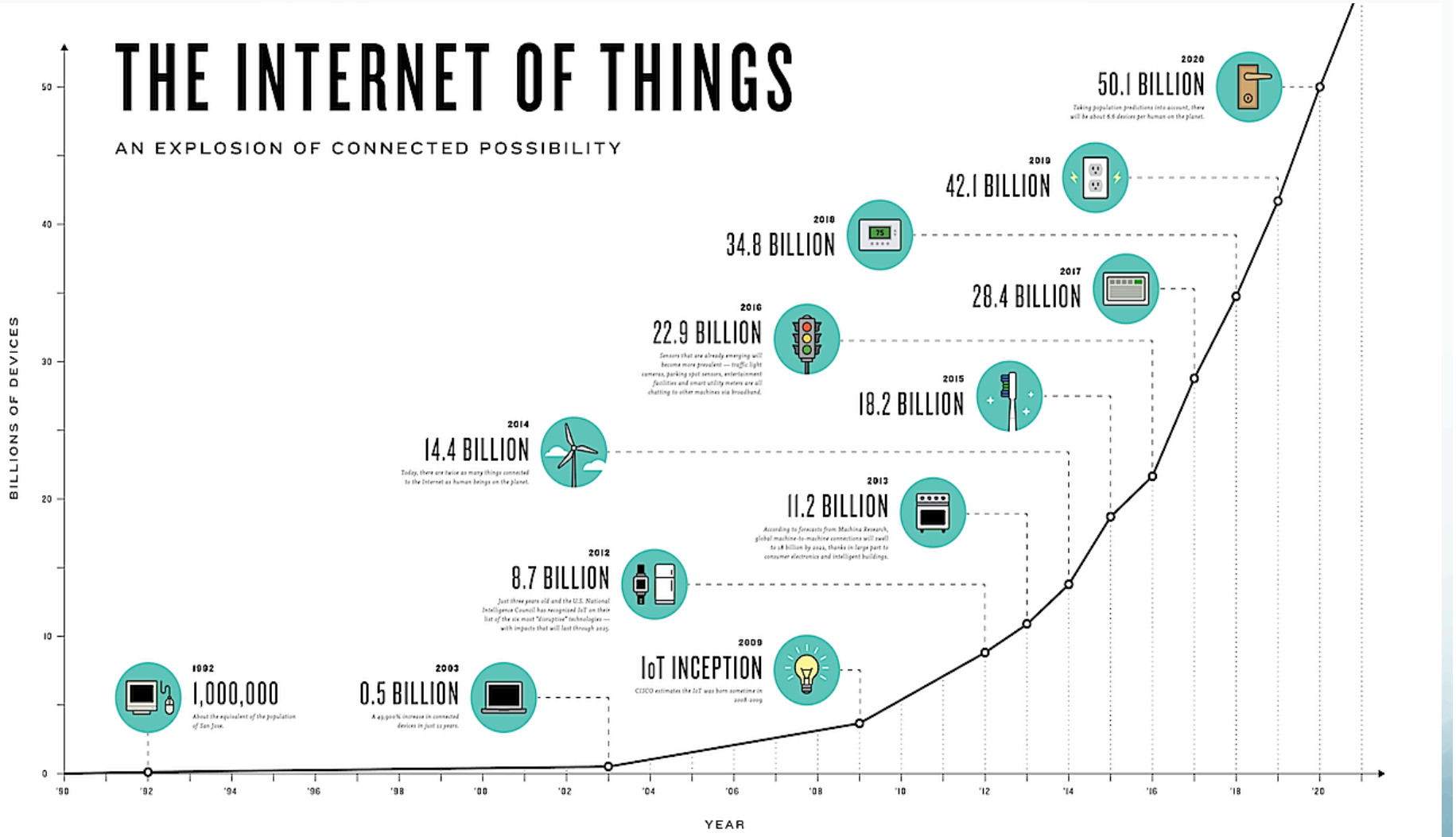
- Social networking
- Cloud services
- BYOD
- Big Data and Analytics
- Siri, Cortana, and Alexa
- Continuous information gathering by:
  - Your car
  - Your house
  - Your watch
  - Your mattress
  - Your toothbrush

Seriously...

Tele-diagnostic Breakthrough

- Your toilet:
  - High PSA
  - Pregnancy
  - GI bacteria
  - Occult GI bleed
  - STI
  - Blood sugar
  - Cholesterol
  - Recreational substances

Ref. The Toilet and Its Role In the Internet of Things. WIRED, April 2014


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
YEAR
1992
1,000,000
About the equivalent of the population of San Jose.
2003
0.5 BILLION
A 49,900% increase in connected devices in just 11 years.
2009
IoT INCEPTION
CISCO estimates the IoT was born sometime in 2008-2009
2012
8.7 BILLION
Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.
2013
11.2 BILLION
According to forecasts from Machina Research, global machine-to-machine connections will swell to 18 billion by 2022, thanks in large part to consumer electronics and intelligent buildings.
2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.
2015
18.2 BILLION
2016
22.9 BILLION
Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all chatting to other machines via broadband.
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION
Taking population predictions into account, there will be about 6.6 devices per human on the planet.

Solve's Perspective

So how far off course are we?

Privacy

Principle	Status
Your information is yours to control – you can share it and unshare it.	• Unsharing is problematic. Few organizations have policy or procedure for "forgetting" you
You share your information with specified individuals for specific purposes by consent only.	• Not all collection is by explicit consent – some informed implied consent, some no consent at all • Health information legislation allows disclosure without consent • Some legislation allows conditional disclosure for research
By default your consent is set to "No"…	• Once you data is in the hands of of a custodian this principle can be suspended
Control access and disclosure	• Mistaken attempts to hand off privacy accountability to service providers • Multi-million record breaches • Multi-billion dollar expenses • Failure to encrypt
Maintain accuracy	• Errors during collection are common • Information QA is minimal • Big Data leads to big errors
Give you access	• Some do, most don't. (See Access principles)

So how far off course are we?

Access

Principle	Status
Information is managed with access in mind.	• Little evidence to suggest information is classified and managed in a way that supports this principle. • Email purging and sanitizing • Open Government and Open Data initiatives limited to a small fraction of government information • Information Governance
Access is part of doing business	• Many requests routed through FOI process • Reduction in published information
If it's not specifically exempted, it's reasonably accessible.	• The reverse is often the case • Much information excluded without proof of harm • Much information unjustifiably redacted
The custodian assists the requester.	• Few custodians understand access requirements • Central access services may not understand business
Personal information is there when you ask for it.	• From my bank – Yes • From my doctor or hospital – 30 days with access request • Most organization not equipped for timely access

Some US Examples

- Cost of cyber-crime up 82% since 2009.
  - Average cost $7.7M 2015
  - Attack frequency increasing: ca. 50% in 4 years
  - Resolution time increasing: ca. 230% in 6 years
- Government practices ill defined
  - Lack of skills and organization
- Healthcare underfunded and unprepared
- Companies with cyber insurance work harder at protecting information
- Ref.www.poneman.org

And in Canada

- Stupid human tricks are still the the biggest threat
- Lack of leadership and expertise are high on the list of weaknesses
- ¼ of survey organizations (n=623) experience almost one cyber-attack per week
- About half of the attacks result in breach of "sensitive" information
- Training and awareness provides big bang for the buck.

Ref. http://www.ponemon.org/local/upload/file/Scalar%20Report%20FINAL%201.pdf

History Repeats Itself

- **Federal**
  - 1978: Operation Ham 400 warrantless RCMP break-ins and thefts of records between 1970 and 1973.
  - 2016: OSEC: Ongoing unauthorized collection and use of citizen “metadata”.
- **Provincial**
  - 2007: Ministry of Health loss of unencrypted patient information. IPC: Data must be encrypted
  - 2016: Ministry of Education loss of unencrypted student information. IPC: Data must be encrypted

http://www.statewatch.org/news/2014/jul/bits-of-freedom-on-the-metadata-of-your-phone.pdf

Consequences

Privacy

- Loss of personal autonomy/Identity theft
- Steady erosion of trust in public custodians
- Withholding or falsifying information
- Capitulation to demands of the private sector for PI
- Technology vacuums PI out of your everyday life

Access

- Adversarial environment
- Loss of transparency
- Gaps in accountability
- Loss of historical records

Both: Increased Risk and Harms

BLISS informatics

Organization Breach Costs

- Breach incident response costs
- Lost productivity costs
- Consultation time with legal counsel and executive
- Staff time to determine individuals impacted
- Staff time to collect contact information for impacted customers
- Client contact costs
- Call centres to respond to client questions and concerns
- Cost for credit monitoring for 3 – 5 years
- Cost of forensic and criminal investigations
- Cost to change/repair/replace information system
- Fines and fees mandated by legislation
- Legal awards to clients
- Legal awards to partners
- Legal fees for defence
- Legal fees for tort prosecution
- Cost of lost business
- Cost of investor relations management
- Cost of replacement executive search and recruitment

Breach cost calculator: http://www.informationshield.com/privacybreachcalc.html

Breach Litigation

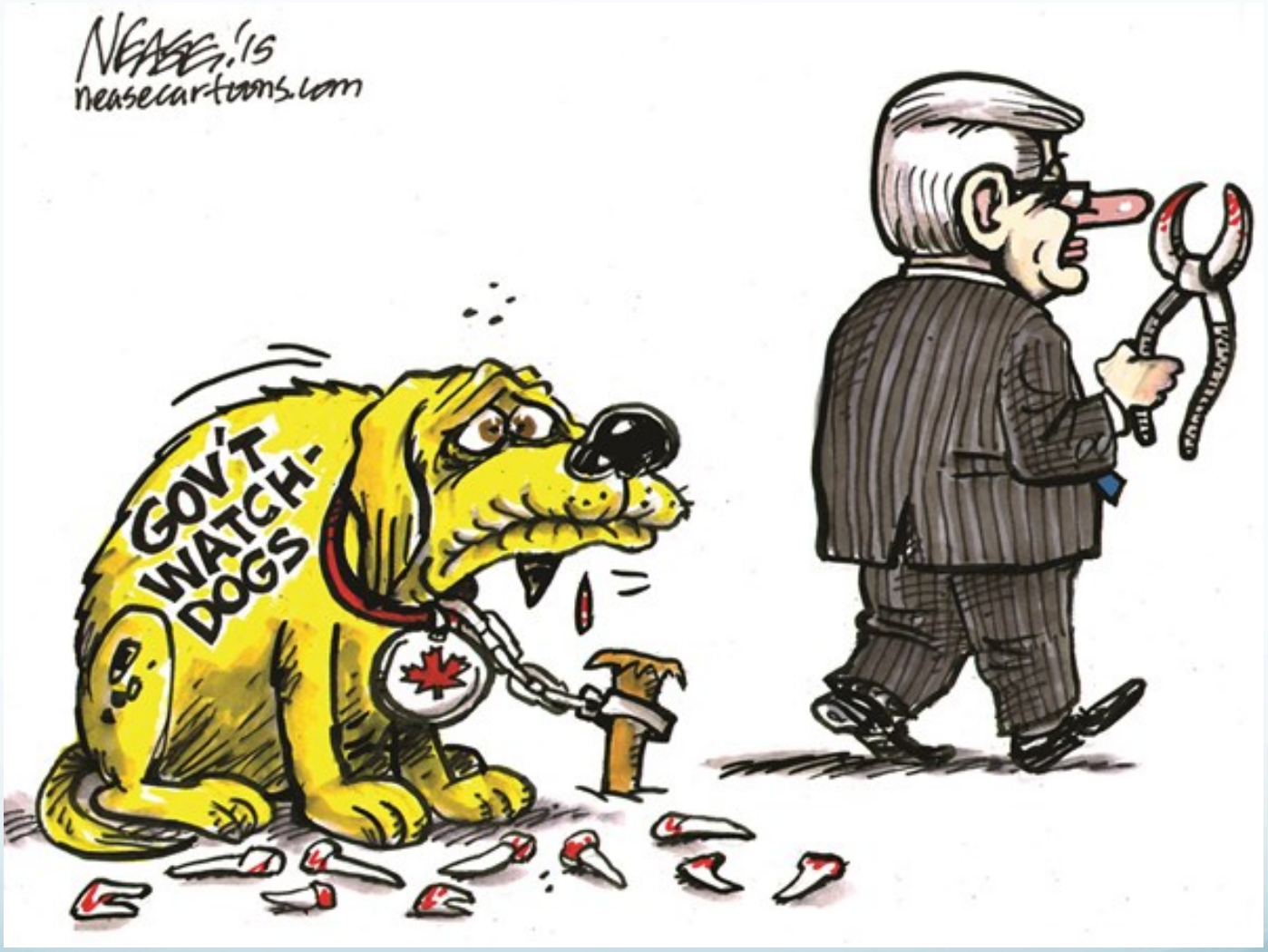
Every province, every state, Target, Sony Films, Ashley Madison, Sony PlayStation, UVic, Home Depot, iCloud, Wendy's, Hyatt Hotels, Time Warner Cable, Aspire Health, 191 million voter records-unknown source

Ref. Privacy Rights Clearing House
http://www.privacyrights.org/data-breach/new

Ref. Merchant Law http://www.merchantlaw.com/class-actions

Why?

- Toothless watchdogs
- Inadequate education – gaps in understanding
- Torts take time
- Downsizing
- “Oral” government
- Political expedience/Human nature
- Gaps in IT requirements specifications – PbD and AbD generally MIA
- Challenges in the legislation


NEASE '15
neasecartoons.com
GOV'T WATCH-DOGS

Toothless Watchdogs

- Blocked from Bill C-51 consultation process
- Missing requirements for breach reporting
- Legislative change implementation gaps
- Missing ruling enforcement authority
- Limited monetary penalties
- Conflict with civil and state security organizations
- Political nature of the position

Education/Understanding

- Copy/Paste of legislation wording
- Not tailored for audience
- Missing role relevant definitions and examples
- Lack of understanding of fundamental principles
- Lack of clarity in legislation
- Tone-at-the-Top


We take privacy very seriously here.
BONK

The Civil Legal System

- Civil litigation is expensive
- Tort litigation takes a long time (4 – 5 years)
- Class action takes a really long time (8 – 12 years)
- Inconsistent judgment rulings
- No breach notification
- Few individuals understand their rights

Downsizing

- Almost two decades of organizational rationalization
- Outsourcing removes process knowledge
- Corporate intelligence leaves with retirees
- Much undocumented process is lost
- Knowledge gaps take time to reveal themselves in process failures.
- The audit and oversight function is often the first to get chopped.

Oral Government

- Records management gap – paper to IT
- Downsizing
- Creative interpretation of legislation
- Organizational churn
- No replacement of discontinued publications
- Nascent Information Governance agenda
- BC IM Act/Chief Records Officer

Human Nature

- Aversion to criticism drives government access gap
- Knowledge gaps increases accident probability
- Leadership and accountability vacuum

IT Culture and Practice

- PMs and scope creep
- Privacy and security rarely specified as explicit requirements
- Security often mistaken for privacy
- Outsourcing and Cloud initiatives often overlooked
- Privacy perceived as a compliance add-on

Gaps in Legislation

- Limited or missing penalties
- Weak and missing enforcement
- Gaps from changing technology
- Gaps from changing business processes
- Watchdog resourcing
- Legislator education gap

Nobody escapes surveillance

How do we fix it?

- Most privacy legislation has a revision cycle built-in
- Generally, Privacy Commissioners and invited interested parties contribute recommendations
- Anyone can submit recommendations as a rule
- Review process does not guarantee revision of the legislation
- Most privacy legislation has undergone at least one revision cycle
- Two examples of legislation remediation recommendations…

1987 “Open and Shut”

- First legally mandated review of first Access and Privacy legislation in Canada (1983, the year after the Canadian Charter of Rights and Freedoms)
- Regarded as a fundamental underpinning of Canadian democracy
- Both acts were found to have major shortcomings and weaknesses:
  - Lack of awareness and education
  - Access delays and database exemptions
  - Insufficient support by senior management
  - Scope and definition issues with “personal information” , “consistent use/ purpose”, exemptions
  - No privacy protection (security) framework
  - Gaps due to the increasing power of IT, data linkage, cross border flows

1987 Recommendations

- Strengthen monitoring and enforcement including penalties
- Extend and clarify organizations covered
- Duty to record
- Proactive disclosure by design/exemption only for harm
- Requirement for privacy management program
- Mandatory breach notification
- Accountability requirement

Recommendations from 2014 BC PIPA Review

"…we have witnessed a staggering escalation in the volume of personal information that organizations collect from British Columbians."

- Emphasize Accountability:

  Def. "An organization accepting and being able to demonstrate responsibility for personal information under its control."

- Mandatory breach notification with $100,000 non-compliance penalty
- Expressly state accountability belongs to the original custodian/collector and not to third party service providers
- Require custodians audit third party service providers (operations, cloud, analytics) for compliance capability
- Mandated privacy management program with employee education and regular monitoring and update cycles
- Mandate transparency logging and reporting for non-consensual disclosures
- Add order making powers for commissioner initiated investigations

Conclusion

- Privacy legislation appears to be broken
- Recent recommendations overlap substantially with recommendations from 29 years ago
- The existing repair process doesn't appear to be working
- The risks and control failures are increasing in scale and frequency
- Is it time to go back to the ethical principles for a reset?...

Today

- BC FIPPA review closed last week.
- Privacy PIPPA legislation review open in Alberta. Participate through PACC or independently.
- New Newfoundland ATIPP act supports principle of default access to government information.
- NWT ATIPP review emphasizes Health Information Act consent clarification and accountability education.
- NWT Power provides textbook privacy breach response.
- HIPAA reinforces right of patient access

Federal Ministerial Mandates

The Leader of the House of Commons is to Work with the President of the Treasury Board and the Minister of Justice and Attorney General to enhance the openness of government, including:

1. Supporting a review of the Access to Information Act to ensure that Canadians have easier access to their own personal information
2. That the Information Commissioner is empowered to order government information to be released
3. That the Act applies appropriately to the Prime Minister's and Ministers' Offices, as well as administrative institutions that support Parliament and the courts.

Some Goals to Consider

1. Update Privacy laws to clearly mandate individual access to their personal information as a part of basic business services.
2. Update Access laws to mandate timely reasonable access to all organizational information except categories exempted by a harms test.
3. Get back to the basics of recordkeeping. Require the implementation of information governance processes and standards.
4. Education: More and better training, refreshed annually. From the board of directors to the office temp.

Remember…

Ref. Red Green

BLISS informatics

Thank You!