

DATA PRIVACY

RISK

LAW

PROTECTION

COMPLIANCE

REGULATIONS

EXPOSED

RECORD

breach

data

digital

classification

search

Metadata

anonymous

Privacy

Patient privacy

Sensitive Information

Authentication

Agenda – Privacy On the Internet

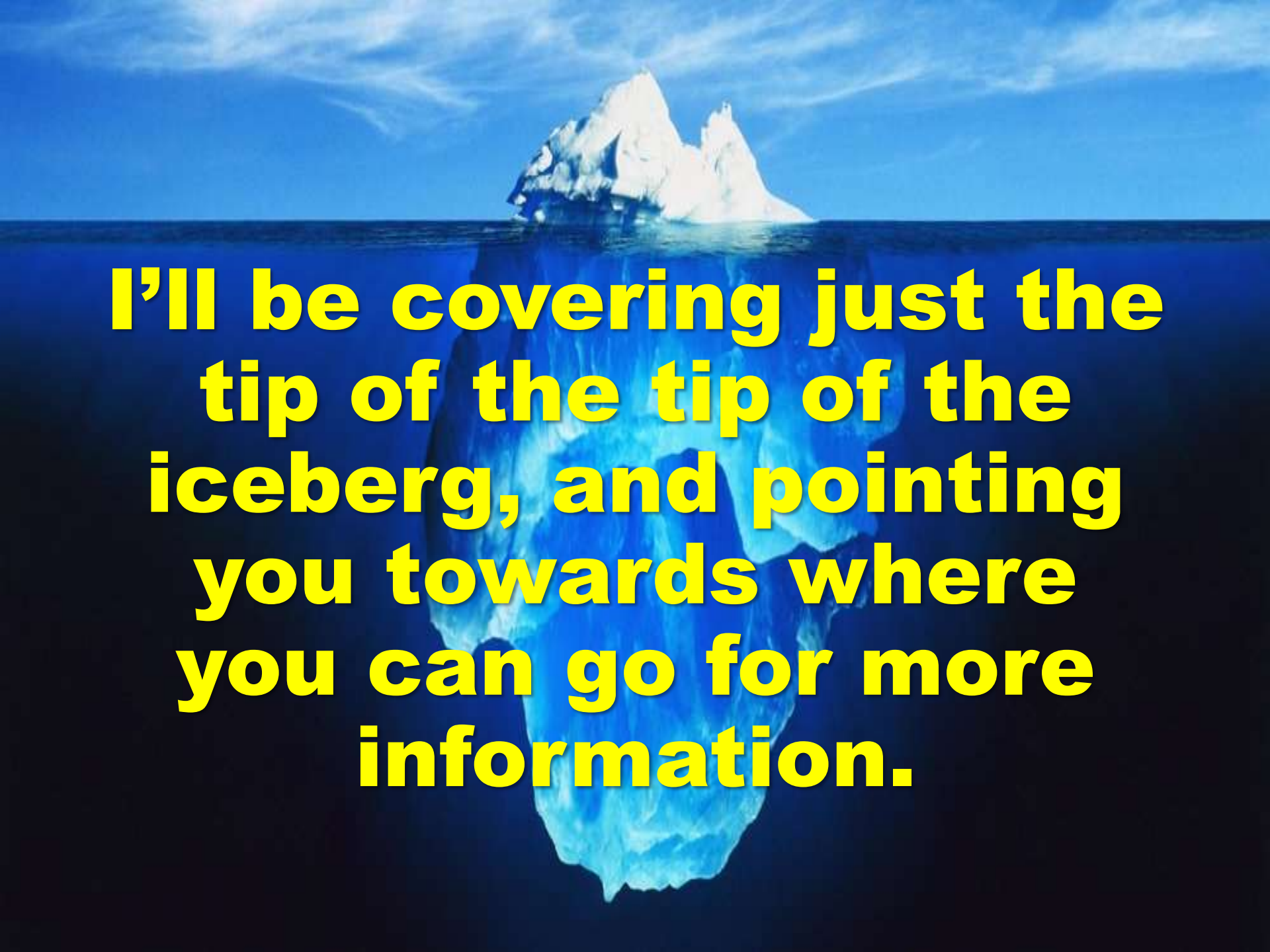
- A few weeks ago Tom Trottier gave a great presentation on security and security layers.
- Over the last couple of weeks we've looked at VPN's (Virtual Private Networks), including their role in internet privacy and security.
- This week we're going to kick off a mini-series on

Internet Privacy

and tonight we're going to start it off by looking at WHY you need to guard your privacy online.

- In future weeks we'll look at:
 - Browsers and basic browser privacy settings
 - Search engines
 - Some of the ways you can be tracked
 - Anti-tracking and add blocker software

Then we'll see where we go from there

A photograph of a large iceberg floating in the ocean. The iceberg is white and jagged, with a prominent peak. The water is a deep blue, and the sky is a lighter blue with some wispy clouds. The iceberg's reflection is visible in the water below the surface.

I'll be covering just the tip of the tip of the iceberg, and pointing you towards where you can go for more information.

Privacy vs. Security



vs.



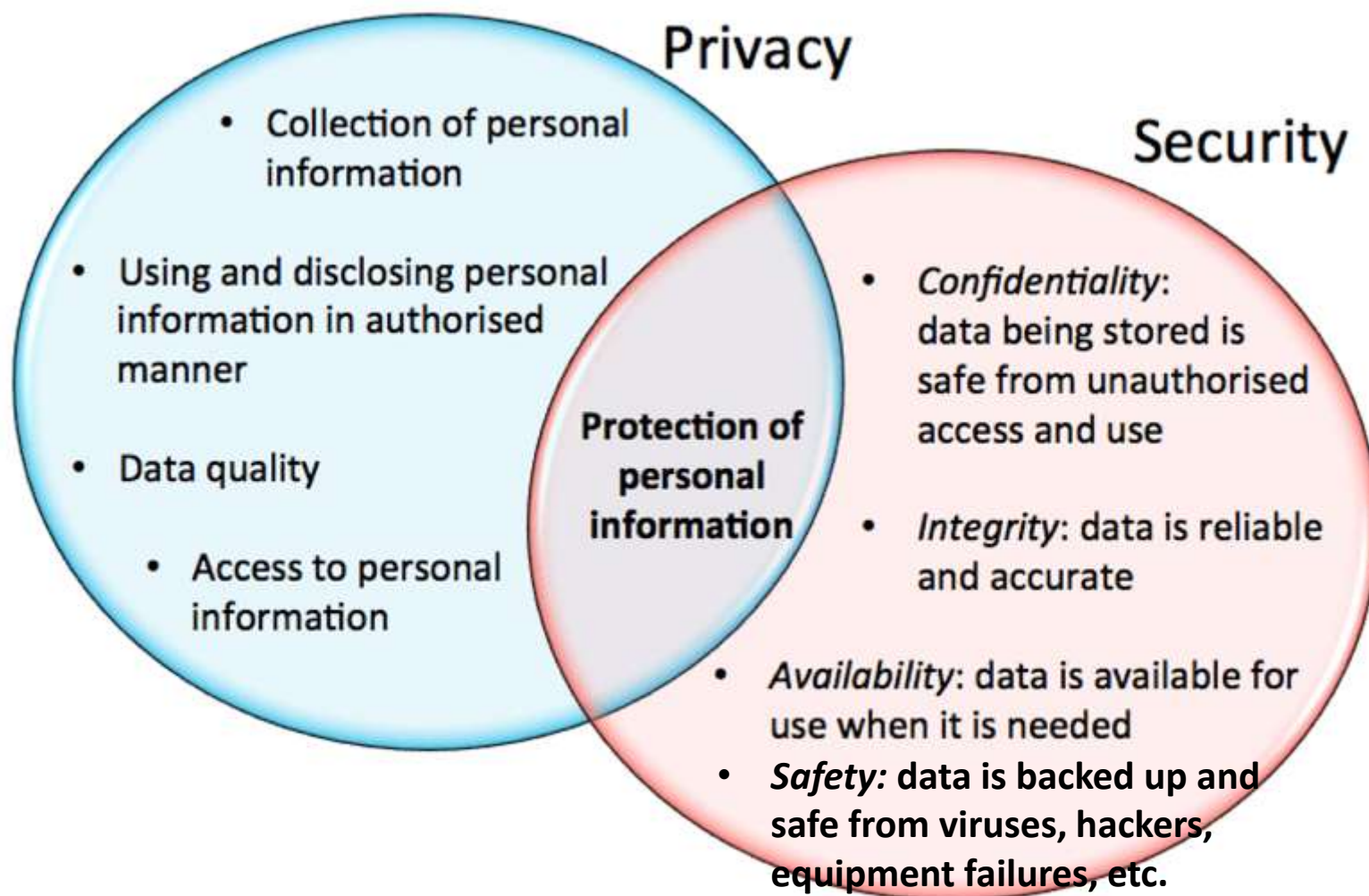
**IS YOUR
DATA
PRIVATE?**

vs.

**IS YOUR
DATA
SAFE?**

DATA = INFORMATION

Privacy and Security Overlap



Privacy Concerns

If your internet activity is pretty vanilla then privacy (as opposed to security) might not be a BIG concern for you. But if you:

- **Use Facebook or other social media a lot**
- **Have skeletons from your past hidden in your closet**
- **Are involved in any political, human rights or protest activities**
- **Have health issues you don't want your employer or insurance companies to know about**
- **Are applying for a job at a large company or organization**
- **Download pirated music, movies, etc.**
- **Go to adult websites**
- **Etc., etc., etc.**

Then you need to take your online privacy seriously.

I'M GLAD FACEBOOKS
TAKING PRIVACY ISSUES
SERIOUSLY...

NUDIST, MARRIED, 75K ANNUALLY,
DRINKER, MINIVAN OWNER,
BEANIE BABY COLLECTOR...

Mike Luckovich
ALL JOHN DEERE
ILLUSTRATIONS
© 2004



The Threats

- **Google trackers are present on 82% of the web traffic.**
- **25% of the web has a hidden Facebook tracking pixel. Facebook knows a lot more than just what you do on Facebook.**
- **A third of the 6000 top websites have more than 10 trackers per page.**

The Threats

Many companies, including internet giants Google and Facebook, make most of their money by using your personal information for targeting advertising or by selling your personal information to advertisers, insurance companies and others.

Other internet companies from giants like Amazon to maandpa.com to everything in between also make some of their money selling your personal information.

The Threats

Don't forget that as well as the Chrome browser and Gmail, that the Android operating system on your smartphone, tablet or Chromebook is a Google product.

And let's not forget Google Home, Maps, Calendar, Images, Earth, Streetview, Translate, Drive, Play, etc.,

Oh yeah, and other Google properties like YouTube, Motorola Mobility, Nest, DoubleClick, Fitbit, etc.

The Threats

By default, most Google privacy valves are opened up to the max, and navigating the layers of settings, not only with Google itself but also with the various third-party services that interact with your phone, is often easier said than done.

For Android, look at this article for a start:

<https://www.computerworld.com/article/3545530/ultimate-guide-to-privacy-on-android.html>

What Google Knows

If you use Google as your search engine and Gmail as your email client, Android devices, Google Apps or other Google associated properties like YouTube, and many non-Google sites, Google tracks:

- every search you make and what sites you click through to,
- what sites you visit, what pages on the sites you go to and how long you're there,
- what you copy or download,
- who you communicate with,
- what the contents of your emails are, what attachments and links you send,
- what online shopping you do and what you buy,
- Google tracking on your smartphone knows all of your comings and goings, where you've been and for how long.
- etc., etc., etc.

Even if you DON'T use Google as your search engine and Gmail as your email client, Google tracks you in many other ways.

What Google Knows

An example:

Your picture can be posted in your Facebook profile, in a friend's Facebook post on the great drunken party you were at or the political protest demonstration you attended, in a news article about your charity work or your arrest or your house fire, on any website or in a blog, in an email, or pretty much anywhere on the internet, and it can end up in places like Google Images for anyone to see and use.



What Amazon Knows

From an Ottawa Citizen story

Ibraheem Samirah, a Democratic member of the Virginia House of Delegates, was stunned to learn the full details of the information Amazon has collected on him, including:

- More than 1,000 contacts from his phone
- Exactly which part of the Quran that he had listened to on Dec. 17 of last year.
- Every search he had made on Amazon, including one for books on "*progressive community organizing*" and other sensitive health-related inquiries he thought were private.

"Are they selling products, or are they spying on everyday people?"

<https://ottawacitizen.com/pmnl/business-pmnl/a-look-at-the-intimate-details-amazon-knows-about-us/wcm/815e90e7-0563-4d03-a14a-da04d6ca13fd>

As well as tracking what you look at and buy on Amazon, they collect data through:

- **their Alexa/Echo/Ring/etc. smart home products,**
- **their e-commerce marketplace,**
- **Kindle e-readers and Kindle apps,**
- **Audible audiobooks,**
- **their video and music platforms,**
- **home-security cameras,**
- **fitness trackers,**
- **their many online products**

Alexa-enabled devices make recordings inside people's homes, and Ring and Wyze security cameras capture every visitor (gadzooks, what if you have these cameras INSIDE your home?).

Such information can reveal a person's height, weight and health; their ethnicity (via clues contained in voice data) and political leanings; their reading and buying habits; their whereabouts on any given day, and sometimes whom they have met with.

The Threats

If something on the internet is free, if you are not paying for it, then you are not the customer;

**YOU ARE THE
PRODUCT BEING
SOLD!!!**

The Threats

Even if you ARE paying for the product or service (e.g. Amazon),

THEN YOU ARE STILL

JUST ANOTHER

PRODUCT BEING

SOLD!!!

The Threats

Google, Facebook, Amazon, et al, want you to live your life online and in the cloud so that they can know everything about you, no matter how personal, and the more they know the more they can sell.

The Threats



Dubbed "*the new oil*", data is fast becoming one of the most valuable resources on Earth

The Threats

But if you've been using the internet for years, isn't that horse already out of the barn?



The Threats

There's not much you can do about the info they already have, but you can make it harder for them to get any more, starting with:

- The browser(s) you use and the browser privacy settings**
- The search engines you use**
- Using anti-tracking and add blocker software**
- Being aware of the threats**

The Threats

There are companies that can try to remove specific information about you from the internet, but it's like a five dimensional game of Whack-a-Mole.



Genetic Testing

Companies that do genetic testing for ancestry tracing and health information like Ancestry DNA and 23andMe share some of their data with pharmaceutical companies and other organizations doing genetic research.

There are 'opt out' clauses to the sharing of your data, but they may be hard to find, and you may want to dig deeper into their privacy policies before you use these services.

Note that data shared can be 'anonymized' (i.e. no personal identifiers) or can be specific to a particular person.

Passing Your Information On

An example of third party data sharing:

Do you know what the privacy policies of your bank(s) and credit card companies are?

You know they share data about you with credit reporting agencies, but who do the credit reporting agencies share that data with, and who do those they share it with share it with, and so on?

What are governments doing?

- The Canadian government is *'very concerned about the privacy of its citizens'* but is doing very little about those concerns, the American government is even worse.
- The EU (European Union) is somewhat better but still inadequate in protecting its citizen's privacy.
- The Chinese, Russian, North Korean and other governments are actively involved in hacking, spying, ransomware, cyber warfare, selling hacked information like social insurance numbers and more to the badies, etc.
- With the internet massively crossing international boundaries, what can really be effectively done?

What are governments doing?

Should these companies and organizations be required to:

- Post their privacy policies where they are easy to find, and written in clear, simple, concise, non-Harvard Law School language the average person can easily understand.**
- Allow their users and customers to EASILY opt out of sharing some or all of their personal information.**
- Have their default privacy settings set to the maximum instead of the minimum**

**Most of the companies, organizations
and governments dealing with your
personal information DON'T have your
best interests at heart.**

**Unfortunately, just like your security,
your PRIVACY, both on and off line, is up
to **YOU!****





We've looked at some of the reasons you need to be concerned about your privacy.

Next time we'll start looking at what you can do to protect your privacy, starting with a look at browsers and basic browser privacy settings.

In the meantime, have a look at this:

<https://defendingdigital.com/best-anti-tracking-software/>