# PRIVACY, TRACKING AND THE "INTERNET OF THINGS"

Big Brother is alive, well and watching what you do…

October 2016
Security Awareness Team
IT Services

Royal Roads UNIVERSITY

# TODAY'S AGENDA

- We're NOT here to:
  - Scare you
  - Tell you what to do
    - Privacy is personal and each person's "limits" are different
    - Workplace privacy is different – here we're bound by legislation!
- We ARE here to
  - Acquaint you with some of what's happening on the Internet
  - Give you some suggestions about staying safe and guarding your privacy
  - BRIEFLY talk about privacy in the workplace

# WE’RE GOING TO TALK ABOUT….

- Privacy on the Internet – how DO they know so much about you?
- The “Internet of Things” – the shape of things to come?
- Privacy in the workplace – FIPPA, CASL and all that.

Let’s get started…

# THE WORLD-WIDE WEB – BIG BROTHER’S PLAYGROUND

# IS IT REALLY “FREE”?

- How many Facebook users in the room today?
- How much do you pay for your Facebook account?

Consider:

- In 2014, Facebook paid 19 BILLION dollars for “WhatsApp”, the popular messaging app, and another 2 BILLION for Oculus VR, a virtual reality technology.
- Where does the money come from???

*highly targeted, personalised advertising*

- How does advertising become "highly targeted" and "personalised"?
  - By tracking what you do and building a profile of YOU

YOU are the product

# PRIVACY ON THE WEB

- There isn't any!  :^)
- The Internet these days is a trade-off of giving up bits of personal information in exchange for the information you want.
- When looking at Privacy you need to consider:
  - Tracking (cookies, etc.)
  - Privacy policies
  - How your data is being used
- Remember – the Web is forever…

Let's look at some of the issues

# HOW ARE WE TRACKED?

Many different methods are used to collect information on what we do on the internet – here's a few common methods:

Cookies:

- Small files, called "cookies", placed on your computer when you visit a site.

- Websites use cookies to track a variety of things related to your interaction with the site.
  - Cookies may track such things as
    - Your site preferences
    - Pages that you visited
    - Links that you clicked on
    - Etc.

# OTHER TRACKING METHODS

- Information we provide when signing up for social media sites
- What we search is tracked by some search engines
- When we click on ads or on “marginal content” on websites
- Certain web-based email providers scan our emails.

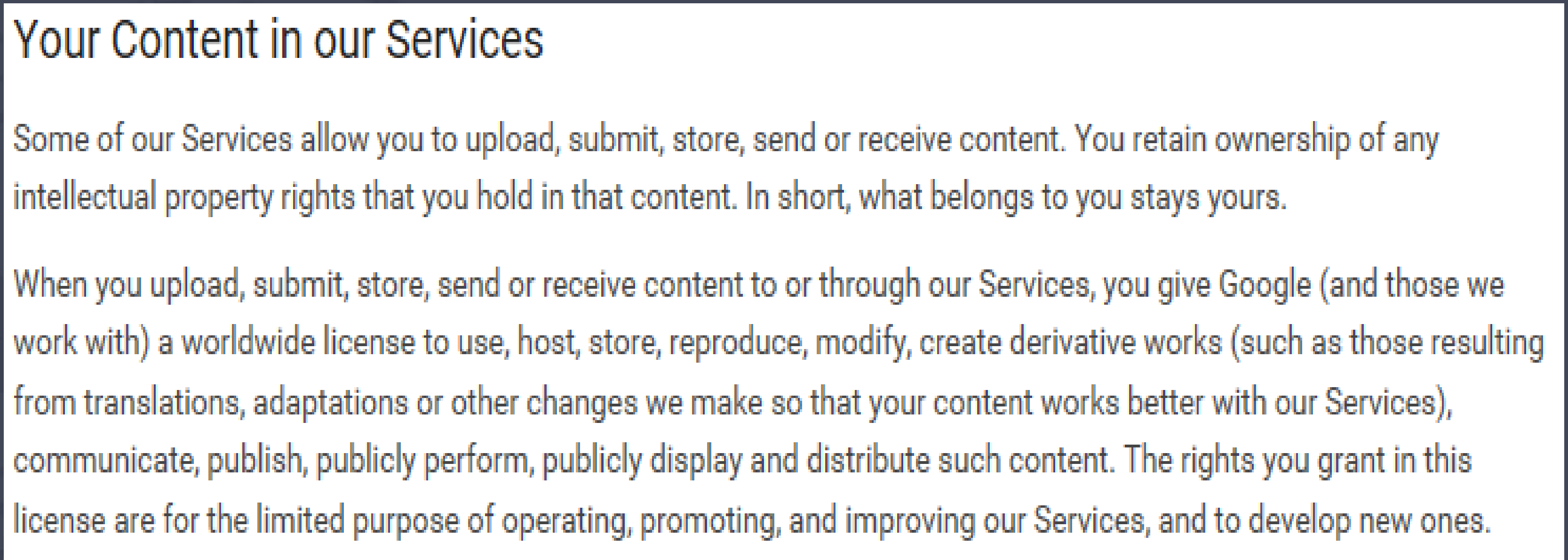
# TRACKING DEMO…

- What sites do you routinely visit? We’ll show you what is happening behind the scenes as you connect to them.

# PRIVACY POLICIES

- Who wants to read all that legalese gobbledy-gook anyway….
  - YOU DO!
- Depending on the jurisdiction privacy policies may or may not be required. Some jurisdictions (UK / EU primarily) even require a cookies policy.
- You need to be aware what sites are doing with the data they capture from you.
  - Read Google's Terms of Use to see what they can do with data you upload
  - What about the photos you upload to Facebook?
  - Etc. etc. etc.

# TERMS OF USE: AN EXAMPLE

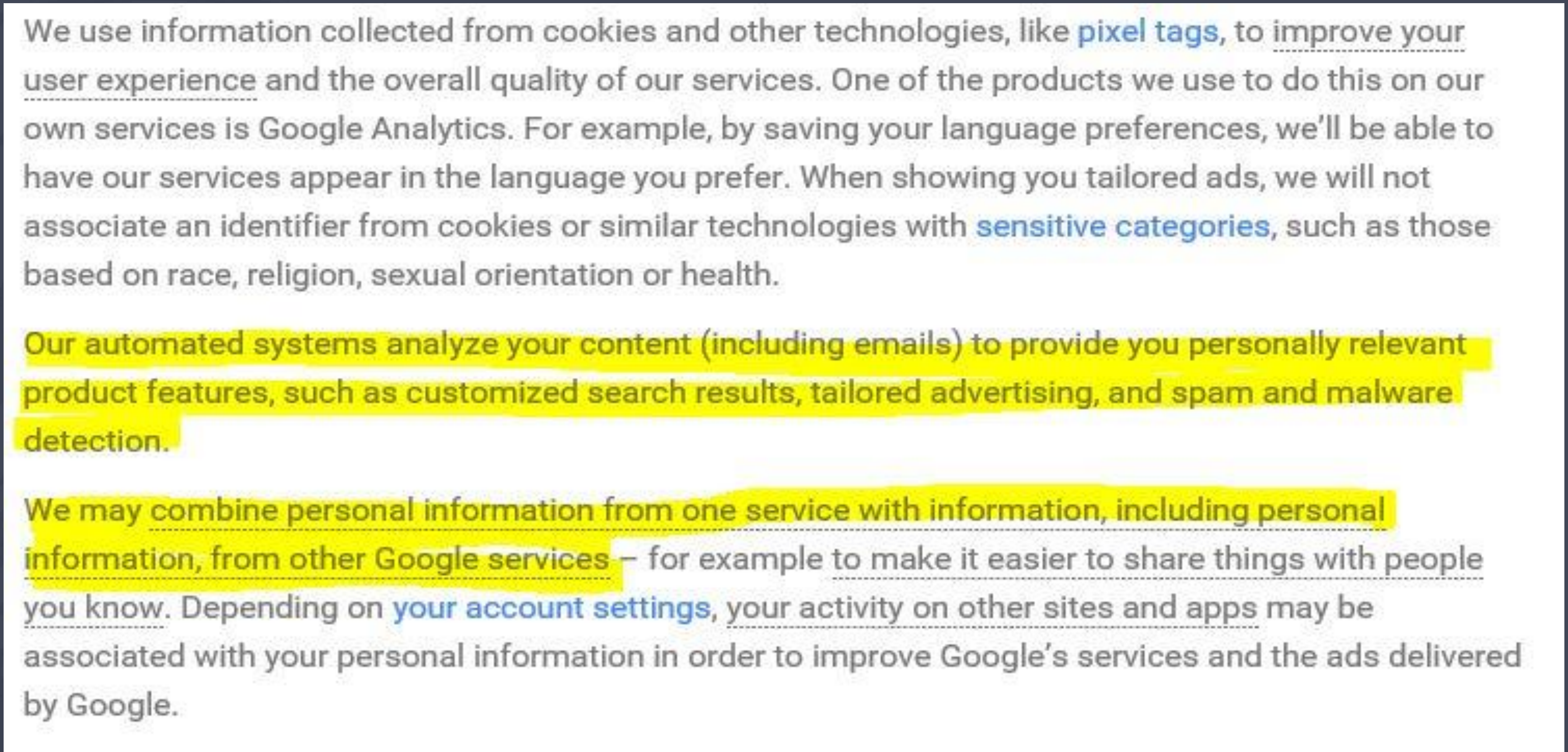


## Your Content in our Services

Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones.

# PRIVACY POLICY: EXAMPLE



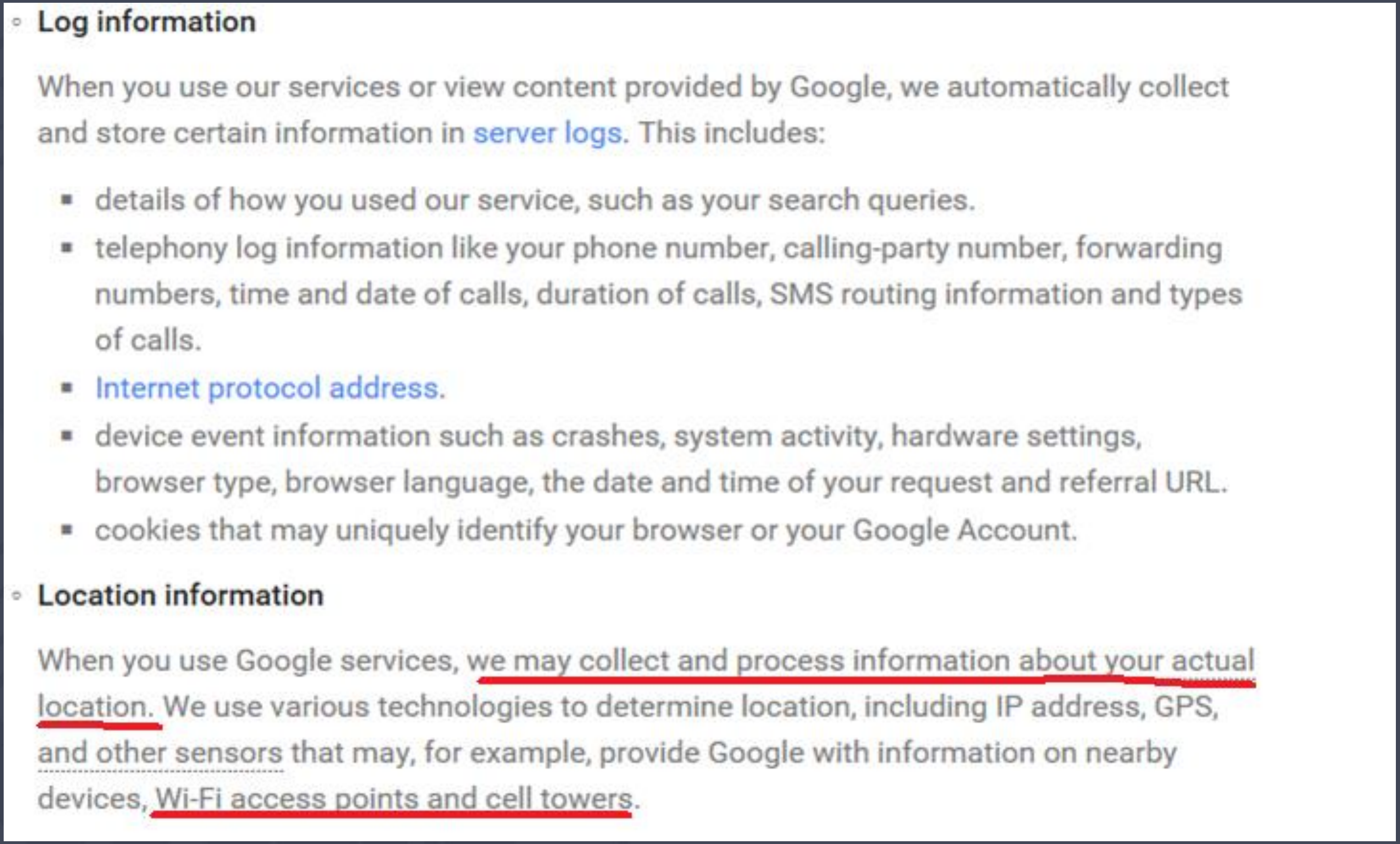
We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

# PRIVACY POLICY EXAMPLE

## CONTINUED…



- **Log information**

  When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:

  - details of how you used our service, such as your search queries.
  - telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
  - Internet protocol address.
  - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
  - cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers.

# PRIVACY BEST PRACTICES

- Many of these suggestions depend on your own comfort level.
- READ  A SITE'S PRIVACY POLICY BEFORE YOU SIGN UP!!!
- Configure your browser to restrict which kinds of cookies you will accept.
- Configure your browser to delete cookies when it closes
  - Note that this will have an impact on your on-line experience
- Consider using a non-tracking search engine like DuckDuckGo or Oscobo
- Be careful with location settings on your devices

# INTERNET OF THINGS

# CONSIDER THE FOLLOWING SCENARIO….

- You’re in your car at the end of the work day, and IT is driving you home.
- You get a text message from your refrigerator at home – apparently you’re out of milk
- You get another text message from your toilet paper dispenser  advising that you’re almost out of TP as well.
- You stop at the store.  As you walk in:
  - You’re caught on their camera system
  - Facial recognition software identifies you
- A notice board displays the message “Welcome Mr. Bloggins”
- Store records reveal that you like Lucky beer.  The same notice board advises that 6 packs of Lucky are on sale! :^)
- Your phone senses you’ve arrived home, and turns on your house lights.

*Welcome to the Internet of Things*

# WHAT IS THE "INTERNET OF THINGS"

- The Internet of Things (IoT) is all about connecting everyday devices to the Internet, for example:
  - Doorbells
  - light bulbs
  - dolls
  - Thermostats

- These connected devices can make our lives much simpler BUT… there are two issues to be concerned with:
  - Security
  - Privacy

*Let's Take a Look*

# INTERNET OF THINGS & SECURITY….

- Many companies making IoT devices:
  - Have little or no experience in IT security
  - Are start-ups focused on getting product to market and not security
  - And so on…

- The result is poorly secured devices that can be
  - Compromised and used for other purposes
  - Leak personal information
  - Expose the user

- A 2014 HP Security Research study determined 70% of these smart IoT connected devices are vulnerable to attack.

# INTERNET OF THINGS & PRIVACY….

Recent Global Privacy Network findings:

*"The privacy communications of internet-connected devices are generally poor and fail to inform users about exactly what personal information is being collected"*

- IoT devices typically collect, share and process data automatically, often with no human intervention.

And now, a quick demo…

# INTERNET OF THINGS – BEST PRACTICES

Increase your security:

- Keep the device off the Internet if possible
- Put the device(s) on a separate network
- Update the device
- Change device passwords and use strong passwords

Protect your privacy:

- Disable any information sharing capabilities
- Supply  the minimum amount of information necessary
  - This includes websites your devices use
- Anonymise the device:
  - "Smith Family Doorbell" is asking for trouble…

# PRIVACY AND THE WORKPLACE

# PRIVACY & THE WORKPLACE – A QUICK LOOK

- A very complex issue, filled with acronyms…FIPPA, CASL, PIPEDA, PIPA, etc.
- Essentially, we need to:
  - Safeguard the personal data in our care
  - Ensure that we are complying with legislation
  - Provide access to the data as appropriate
  - Use the data we've collected only for the purpose stated when the data was collected
  - Collect only the data we need
  - Only collect / use personal information if a person consents

# THOSE ACRONYMS…

- **PIPEDA**
  - Personal Information Protection and Electronic Documents Act
- **PIPA**
  - Personal Information Protection Act
- **FIPPA**
  - Freedom of Information and Protection of Privacy Act
- **CASL**
  - Canada’s Anti-Spam Legislation

# SO, WHAT IS “PERSONAL INFORMATION”?

That’s a good question… it varies depending on the legislation, but essentially personal information is considered to be any information about an *identifiable individual*.

Under FIPPA, personal information is:

- Any recorded information that uniquely identifies you, such as:
  - your name, address, telephone number, age, sex, race, religion, sexual orientation, disability, fingerprints, or blood type.
  - It includes information about your health care, educational, financial, criminal or employment history.
  - It also includes anyone else's opinions about you and your own views or opinions

# WHAT ISN'T PERSONAL INFORMATION?

Again, it varies with the legislation.

Under FIPPA

- **personal information"** means recorded information about an identifiable individual other than *contact information*;
- *Contact information* is:
  - information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual

# COLLECTING PERSONAL INFORMATION

Under FIPPA, a public body can collect personal information if:

- the collection of that information is expressly authorized by or under an Act;
- the information is collected for law enforcement purposes; or
- the information relates directly to and is necessary for the operation of a program or activity of the public body

Consent, identified purpose, etc. all still applies

# OTHER CONSIDERATIONS:

- **FIPPA 30.1** A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:
  - (a) if the individual the information is about has identified the information and has consented to it being stored in another jurisdiction;
- We have a duty to safeguard personal data. This extends to data on laptops, memory sticks, etc. These devices MUST be encrypted.
- FIPPA limits how long we can retain personal information.
- A current or proposed enactment, system, project, program or activity requires a *Privacy Impact Assessment*. (sec 69.1)

# CASL

- Office of the Privacy Commissioner & CRTC share responsibility for CASL
- Organizations are accountable for how they collect, use and disclose personal information, including electronic addresses, in the course of their commercial activities.
  - This includes ensuring that they have obtained informed consent to collect and use individuals' electronic addresses
  - We are responsible under PIPEDA for ensuring that appropriate consent was obtained
  - Consent is implied when the sender and recipient have an existing business relationship
- Every "Commercial Electronic Message" must contain an unsubscribe mechanism that allows the recipient to immediately unsubscribe, at no cost.
- Penalties for violating CASL can be quite large.

# QUESTIONS?