CAN YOUR WEB BROWSER KEEP A SECRET?

Terry Labach
CAN YOUR WEB BROWSER KEEP A SECRET?

NO
QUESTIONS?
BROWSERS

• Desktop
  - Firefox (Windows, Macintosh, Linux)
  - Internet Explorer (Windows)
  - Safari (Macintosh)
  - Chrome (Windows, Macintosh, Linux)
  - Opera (Windows, Macintosh, Linux)
  - WhiteHat Aviator (Windows, Macintosh)
BROWSERS

• Mobile
  - Firefox (Android)
  - Dolphin (Android, iPhone)
  - Internet Explorer (Windows Phone)
  - Metro (Windows Phone)
  - Atomic (iPhone)
  - Chrome (Android, iPhone)
  - Safari (iPhone)
  - Opera (Android, iPhone, Windows Phone)
“My political philosophy is: anything smaller than me is cute; anything bigger than me is scary - elephants, the ocean, Microsoft, the IRS, the IRA, IBM, ICBMs, committees and other mobs, Rush Limbaugh.”

- Michael Swaine, Dr. Dobb's Journal
THREATS TO YOUR PRIVACY

• Business
• Government
• Criminals
THREATS

• Business and government have not generally been thought of as threats

• We know better now
“We’re looking for a cookie alternative…this is well within the rules and regulations and laws and policies that we have.”
- Rich Harris, chief executive of AddThis, on testing of new tracking techniques designed to be harder to avoid.

“Your online profile is being sold on the web. It's kind of crazy and it's not harmless.”
- Sharon Goott Nissim, Electronic Privacy Information Center
YOU ARE THE PRODUCT

the product is you ...
“If there were one thing that I would ask for discussion on is that there has to be some mechanism of accountability for you to sign on to an Internet account that makes it like a digital fingerprint that identifies it to you sitting behind the computer or something at that time. There are mechanisms to do it, but the Internet is so big and so vast at this point, and it’s worldwide, I’m not sure how that could happen, but that would certainly assist everybody.”

- Scott Naylor of the Ontario Provincial Police testifying at a Canadian Senate committee in Nov. 2014
“When conducting national security investigations, the U.S. Federal Bureau of Investigation can issue a National Security Letter (NSL) to obtain identifying information about a subscriber from telephone and Internet companies. The FBI has the authority to prohibit companies from talking about these requests. But we’ve been trying to find a way to provide more information about the NSLs we get—particularly as people have voiced concerns about the increase in their use since 9/11.”

- Richard Salgado, Google
"We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.... if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place."

- James Comey, FBI Director, Oct. 2014
BILL C-51

- 2015 “anti-terrorism” bill
- Permits broad information sharing across government for wide range of purposes
- CSE included in departments allowed to share data
• Communications Security Establishment (CSE) analyzes records of up to 15 million downloads daily from popular websites
• By law, can’t target Canadians
• Data collected without ensuring “targets” are non-Canadian
“...this is not "surveillance," it's "data collection." They say it is done to keep you safe. They're wrong. There is a huge difference between legal programs, legitimate spying, legitimate law enforcement -- where individuals are targeted based on a reasonable, individualized suspicion -- and these programs of dragnet mass surveillance that put entire populations under an all-seeing eye and save copies forever. These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power.”

- Edward Snowden, December 2013
CITIZENFOUR

- Documentary on Edward Snowden, playing at Princess Cinema in Waterloo

  - Sun, Feb 22, 2015 - 7:00pm
  - Tue, Feb 24, 2015 - 6:45pm
  - Wed, Feb 25, 2015 - 9:15pm
YOU ARE THE TARGET
RISKS TO YOU

• Unintentional release of private information
• Businesses can target and manipulate you
• Financial loss
• Harassment from government and law enforcement
• Embarrassment
• Emotional distress
PRIVATE INFORMATION

- Google, Facebook, Yahoo!, etc. present ads that their analysis indicates might be of interest.
- User could be inadvertently outed based on ads presented.
—Why did yeh ask abou’ Facebook?

—Somethin’ Bertie told me, said Jimmy Sr.—Somethin’ he heard.

—It’s illegal if it’s Bertie.

—No, said Jimmy Sr.—It’s not. It’s f****** immoral but.

- Roddy Doyle, from his novel The Guts
EMBARRASSMENT

- Pop-up ad led to married Facebook user being given Zoosk.com account
- The dating site populated her new account with data from her Facebook profile
BIG DATA DOESN’T FORGET

• OfficeMax sent customer mail addressed to "Mike Seay, Daughter Killed in Car Crash."
  ➢ OfficeMax stated "is a result of a mailing list rented through a third-party provider"

• Globe and Mail report on woman inundated with ads for baby and toddler products, based on Big Data
  ➢ Woman had suffered two miscarriages, unable to stop ads
BIG DATA

• Collection of your data largely unregulated
  ➢ Not like credit industry, where you can request and correct credit reports

• Some data brokers will let you request reports
  ➢ This usually (and ironically) involves disclosing personal data to them so they match your record correctly
DIFFERENTIAL PRICING

• Price discrimination
• Price steering
• Retailers use information about you to alter pricing that you see.
• e.g. Orbitz showed costlier hotel rooms to Mac users after market research showed they tend to spend more money than PC users
THE TRACKERS

- Facebook
- Google
- Twitter
- Quantcast
- ComScore
- Clearspring
- Doubleclick
- Neilsen
- Yahoo
- AppNexus
• Amazon uses your **browsing history** to suggest items

• How?
  - Your previous Amazon searches
  - Similar searches and eventual purchases by other customers

• Sounds like metadata!
Can Your Web Browser Keep a Secret?
LEAKY BROWSERS

• Browsers provide information to remote websites
  ➢ IP address
  ➢ Browser version
  ➢ Computer information
  ➢ Location information

• Reporting tools
  ➢ https://panopticlick.eff.org/
  ➢ http://www.whatismybrowser.com/
  ➢ http://www.whatbrowser.org/
INFORMATION LEAKAGE

- Site with malware can use your browser type to craft an attack
- e.g. browsing with Internet Explorer identifies you as a Windows user
- Functionality might be compromised without cause if browser you use is not formally supported
USER AGENTS

• Passed to web server
• e.g. Windows / IE 11: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)
• User Agent Overrider
  ➢ Firefox
  ➢ transmits arbitrary User Agent values
GEOLOCATION

- Your geographical location can be inferred from your computer
- Not 100% reliable due to errors in records
- Can also be spoofed
PROXIES AND GEOLOCATION

• Route your network traffic through a proxy server
• Various reasons to use proxies
• Can be used to make geolocation believe you are located wherever the proxy server is
• TunnelBear is one popular proxy
Can Your Web Browser Keep a Secret?
TRACKING

• Using unique identifiers, businesses can track your web browsing
• By connecting your browsing habits among sites or comparing with other individuals, trends can be identified to assist the business
COOKIES

• Browsers can store files on behalf of a web site
• Each time that site is visited, the browser sends the cookie back to indicate previous activity
  - logged-in status
  - shopping cart
• Contents stipulated by remote site
• Could leak personal data
• Can be used to track your Web activity
Many browsers offer ways to manage and delete cookies.
Many browsers allow you to prevent the storage of cookies from all or some web sites.
Can also use browser plug-ins for greater power and flexibility.
OTHER TRACKING METHODS

• Tracking organizations responded to cookie blocking and to their desire to collect and collate more information

• Canvas fingerprinting

• Evercookies

• Cookie syncing
CANVAS FINGERPRINTING

• Instructs a Web browser to draw a hidden image
• Each computer draws the image slightly differently, so the images can be used to generate a code to uniquely identify each user’s device.
• Not covered by legislation on cookies
• You can see a visible example of a browser fingerprint
EVERCOOKIES

• A site places cookies or cookie-like data in every location allowed by your browser
• If it finds some cookies missing on subsequent visits, it will recreate them using the cookies that survived

- Standard HTTP cookies
- Local Shared Objects (LSOs) (Flash cookies)
- Silverlight Storage
- Storing in RGB values of auto-generated images
- Web history
- Web cache
- Internet Explorer storage
- HTML5 Storage
COOKIE SYNCING

• Allows businesses to work together
• Invisible redirects and embedded URLs allow multiple businesses to give you cookies, which they link to be able to share your data
LIGHTBEAM (AKA COLLUSION)

- Records your browsing activity and the sites involved
- Creates graphic visualization of sites and connections
Can Your Web Browser Keep a Secret?
DO NOT TRACK

• Browser feature
  ➢ Firefox – Do Not Track
    ▪ transmits a Do Not Track HTTP header
    ▪ requires remote site to honour the request
  ➢ IE – Tracking Protection
    ▪ limits information sent to third party sites by referring to a user’s list of allowed sites
    ▪ applies to entire websites, not individual pages
    ▪ can create or download lists
  ➢ Chrome – Incognito
    ▪ won't leave browsing history and cookies on your computer
CAN YOU TRUST YOUR INTERNET PROVIDER?

• Some jurisdictions mandate Internet filtering
• Your internet service provider (ISP) may configure their network to prevent you from searching Google over an encrypted (https:) connection
• Used in schools and for public Wi-Fi
MAN IN THE MIDDLE (MITM)

• Rogers
  - injects content into web pages to send messages about monthly data usage
  - information cached for 30 days
  - for a while, injected ads into bodies of email messages

• Verizon advertising cookie
  - adds secret HTML header to web browsing done from mobile devices
  - likely other providers do the same
CAN YOU TRUST YOUR COMPUTER MANUFACTURER?

- Computer companies may have partnerships with advertisers
MAN IN THE MIDDLE (MITM)

• Lenovo
  - In 2015, discovered to have installed Superfish software on laptop computers sold
  - Injects third-party ads on Google searches and websites
  - Installs own self-signed security certificate authority, which could allow it to intercept user’s private web traffic
PRIVATE BROWSING

- Mozilla
  - Private Browsing allows you to browse the Internet without saving any information about which sites and pages you’ve visited.

- Internet Explorer
  - When you use InPrivate Browsing, info like passwords, search history, and page history is deleted once you close the tab.
• Every Google search you've ever performed is stored
• Data is correlated to your search data from any other Google services you use.
• Even if you delete a search from your Google history, Google will keep it for their own purposes
PEARLS BEFORE SWINE

BY STEPHAN PASTIS

Hey Dad... why you hiding behind the curtain?

Zeeba neighba has new ally. Super smart guy. Lives in zeeba house. Zeeba turn to heem for answer to everything.

So you're hiding from him?

Of course me hiding. Leesten, son... When guy dat smart, you not know what he do.

Did zebra say his name?

Da Google.

Dad could use a computer class.

You no take me alive, da Google!!
TOR

• The onion routing network
• Transmits your communications around a network run by volunteers all around the world
• Proxy servers hide your chain of connections
• Protects the transport of your data
• Visualization of features
  ➢ https://www.eff.org/pages/tor-and-https
PROTECTING YOUR PRIVACY

• Don’t put personal information in on-line searches
• Don't login to your search engine or related tools
• Block cookies from your search engine
• Use web proxies and anonymizing software like Tor
• Configure browser to avoid tracking
PROTECTING YOUR SEARCHES

• Google users can view and manage their search history at https://www.google.com/history

• Use alternative search engines like DuckDuckGo that do not have user logins and do not save your searches

• Authorities and business can’t get data on you that doesn’t exist
PROTECTING YOUR COMMUNICATIONS

• Web sites can use unencrypted (http:) or encrypted (https:) communications
• https: indicates that the transmission of data occurs using TLS (formerly SSL) encryption
• If a web site allows either, use encrypted communications
• Better if the web site only allows encrypted communications
HIDE YOUR IDENTITY

• Use different browsers
• Use different computers
• Use different IP addresses
• Use fake identities if possible
• Fake your browser identification
ENHANCING YOUR BROWSER

• Variety of additional software to add security and privacy support to browser
  ➢ Adblock Plus
  ➢ Ghostery
  ➢ NoScript
  ➢ Better Privacy
  ➢ HTTPS Everywhere
  ➢ Privacy Badger
  ➢ Disconnect
RESOURCES

• Web
  ➢ Electronic Frontier Foundation
    ▪ https://www.eff.org/
  ➢ MediaSmarts
    ▪ http://mediasmarts.ca
  ➢ Disconnect
    ▪ https://disconnect.me/
  ➢ Edward Snowden’s security hints
  ➢ Freedom of the Press Foundation
    ▪ https://freedom.press
RESOURCES

• Books
  ➢ Dragnet Nation
    ▪ Julia Angwin
  ➢ The Smart Girl's Guide to Privacy
    ▪ Violet Blue

• Television
  ➢ United States of Secrets
INFORMATION SECURITY SERVICES

• IST team
• We will provide custom computer security training to your team or department
• Contact Terry Labach to discuss your security education needs
Can Your Web Browser Keep a Secret?
QUESTIONS?

WHAT ARE YOU LOOKING AT?