



# Privacy Lecture 2

Your private data is  
valuable and, doing a  
Security Audit (cont.)

Dr Suelette Dreyfus  
Department of Computing and Information Systems



1. Your data is valuable to you – and others
  - Dollar vs Data
2. The value of privacy, as provided by security, on society and particularly commerce
  - Some good old fashion hard data about what happens to consumers and commerce relating to security/privacy
3. Australian Privacy Principles - Overview
4. Part 2 of our Privacy Audit continues
5. Bonus Track – Extra Privacy and Security Steps



In every community, there is a necessary balance between the rights of the citizen and **companies**. particularly around privacy



*Is ours out of balance?*



- How much is your personal information worth?
- Question: name 3 characteristics that increase the value of your data?





- **Name a piece of private info available about you that is actually online and is valuable?**
- How could this piece of information be valuable to others? Who do you think could use that information?
  - Institutions? Companies? The government? Your friends and family? Cybercriminals?
- What could they use it for?
- Would those ways of using your data help you? Hurt you? Neither?



[http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft\\_site=falcon](http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon)

Or Search:  
'How much  
is your  
personal  
data worth?'  
and FT

What is your data worth?

The infographic features a central figure with a dashed outline, surrounded by icons representing different data categories: a red silhouette for Demographics, a family group for Family & Health, a house for Property, a soccer ball for Activities, and a shopping cart for Consumer. Below these icons is a horizontal bar divided into five colored segments: red (Demographics), orange (Family & Health), green (Property), blue (Activities), and dark grey (Consumer). The 'Family & Health' segment is highlighted with a yellow border. To the right of the bar, the text '\$0.007' is displayed in large white digits, with 'Current value of my data' written in smaller text below it.

DEMOGRAPHICS FAMILY & HEALTH PROPERTY ACTIVITIES CONSUMER

Data brokers scour public documents, such as birth records and motor vehicle reports, to compile basic data about individuals. It is likely they already know your:

- Age
- Gender
- ZIP code
- Ethnicity
- Education level

Are you a millionaire?

No  
 Yes

What is your job?

Not selected

Are you engaged to be married?

Yes  
 No

Are you?

Recently married  
 Recently divorced  
 Empty nester

\$0.007  
Current value of my data



- Customers want to feel their data is secure from unauthorised access, and their privacy is intact
- Ways of ensuring privacy through better security can be heavy-handed and clunky for the average user
- This puts them off – sometimes leading them to choose less secure options.. Thus risking their privacy
- Two issues: Integrity of the company ‘harvesting’ the data and using it **vs** Integrity/protection of that data from others



# What data does the reseller have?

JAN 22, 2014 @ 12:09 PM

13,291 VIEWS

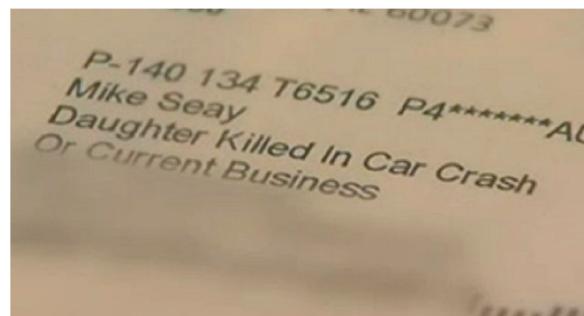
The Little Blac

## OfficeMax Blames Data Broker For 'Daughter Killed in Car Crash' Letter



Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide [FULL BIO](#)



Yikes.

OfficeMax [OMX +%] is getting a lot of press these days and it has little to do with its office supply deals. It was a little too specific in targeting one of its customers, sending a mailing to a Chicago man named Mike Seay addressed to "Daughter Killed in Car Crash or Current Business." Seay's teenage daughter had been killed in a car accident a year earlier, as reported by NBC News. This was obviously traumatic for him.

US Company OfficeMax's #PRFail showed just how much data is gathered and sold on us all – and how very personal it can be.

Advertising mail out to:  
“Daughter Killed in Car Crash or Current Business”  
Seay’s teenage daughter had been killed in a car accident

Hill, K. 2014. 'OfficeMax blames data broker for 'Daughter killed in car crash' letter', *Forbes*, Jan 22. See:  
<http://www.forbes.com/sites/kashmirhill/2014/01/22/officemax-blames-data-broker-for-daughter-killed-in-car-crash-letter/#19458a786b0d>



# Even if the data kept is appropriate, is it secure ‘enough’ for ‘privacy’?

Increasing large scale data breaches .. Leads to:

- Put higher security burdens on clients
- Leads to a diminished user-experience for the customer with the company
- On average, clients must remember more than 14 passwords
- Despite this, consumer perception of security have gotten worse!
- Issues around Digital security and privacy ‘are eroding consumer trust online’

Source: Hasham, S. et al 2016. ‘Is cybersecurity incompatible with digital convenience?’ McKinsey & Co. August. See: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608>



What % of online households reported that concerns about online privacy and security stopped them from:

- Conducting financial transactions
- OR Buying goods or services
- Or posting on social networks
- OR Expressing opinions on controversial or political issues via the internet?



45%

Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>



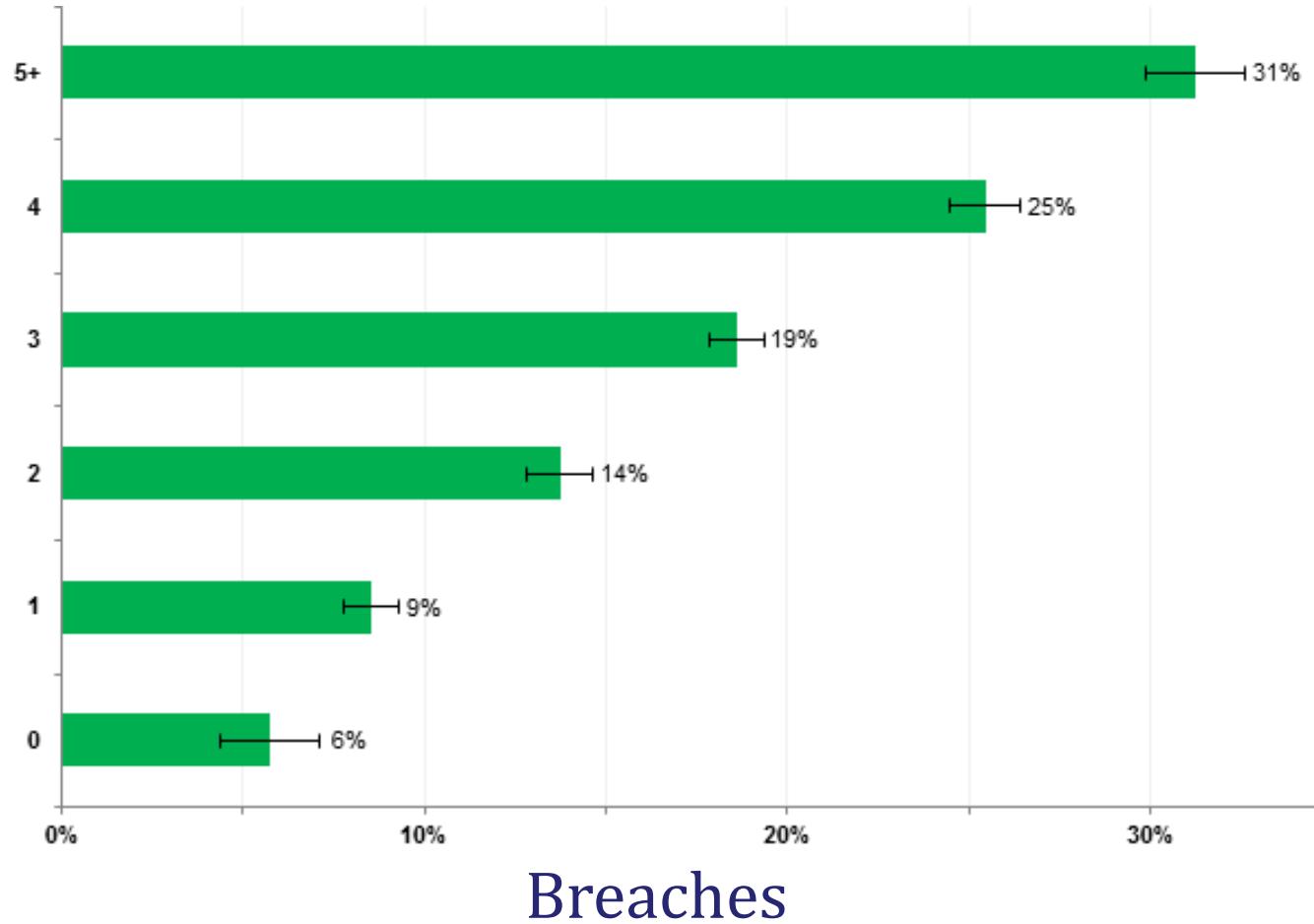
## New realities for consumer behaviour online – Privacy and Security

- 19% of Internet-using households (almost 19 million Americans) reported being impacted by an online security breach, identity theft or similar malicious activity during the 12 months before the July 2015 survey.
- 22% of Internet-using households that used a mobile data plan to go online outside the home experienced an online security breach.
- 84% of households had at least one specific privacy or security concern—and 40% had at least two.

Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>



# of different types of devices used in a household



Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>



# Internet Household reporting online security breaches

“Perhaps the most direct threat to maintaining consumer trust is negative personal experience.”

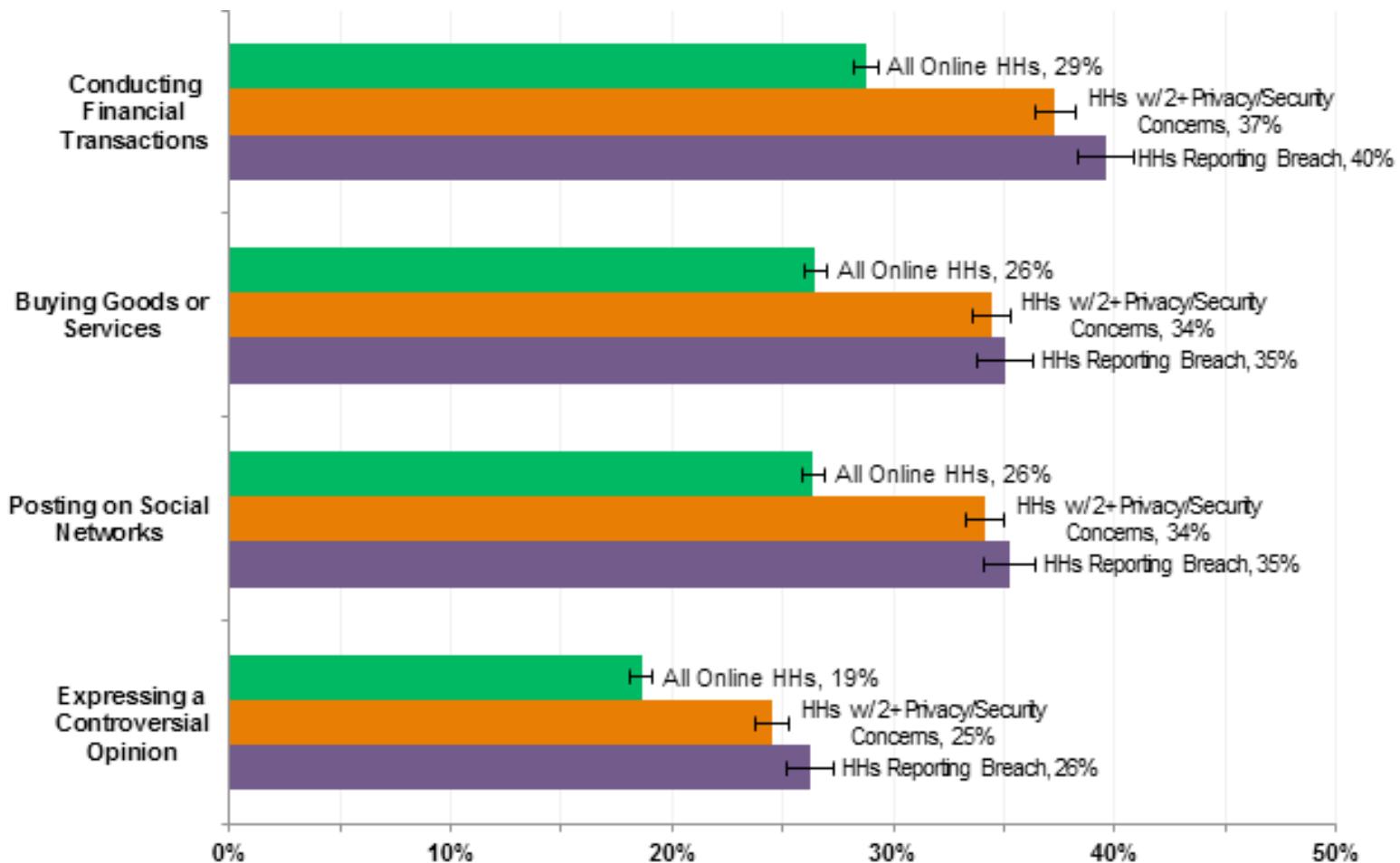
“Security breaches appear to be more common among the most intensive Internet-using households.”

Source: Goldberg, R. 2016. ‘Lack of trust in internet privacy and security may deter economic and other online activities.’ National Telecommunications & Information Administration, US Dept of Commerce. See: <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>



# Avoided online activities due to privacy and security concerns

Types of online transactions  
“HH” are % of households with internet users



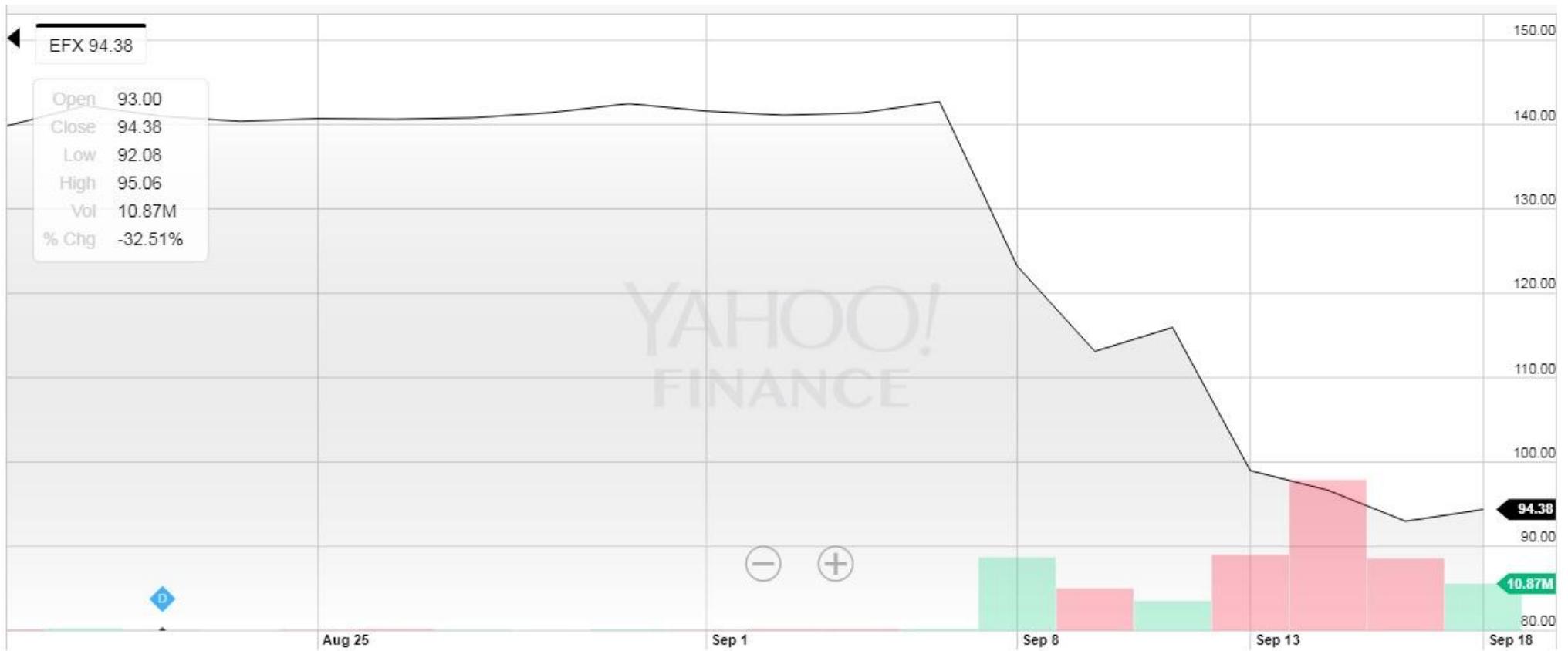
Source: Goldberg, R. 2016. ‘Lack of trust in internet privacy and security may deter economic and other online activities.’ National Telecommunications & Information Administration, US Dept of Commerce. See: <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>. Note: % of households with internet users



- Equifax has said that the breach that exposed sensitive data for as many as 143 million US consumers started on May 13 and lasted until July 30.
- The company didn't disclose the breach until September 7.
- Used a critical vulnerability in the Apache Struts Web app framework – already an exploit in the wild being used at the time – let hackers get foothold
- Known bug, trivial to exploit = reporting of string of attacks in MARCH. Open Source project had patched vulnerability then. 2 x working exploits were publically available.
- PATCH, PATCH, PATCH!



## Case Study: The financial impact of breached data security on a company





# Trade offs between privacy/security and convenience: what customers say in the commercial world

- 30% prioritize ease and convenience over security
- Want ‘basic level’ operating behind the scenes but say ‘having access to account information without the need to enter a password (eg with automatic device recognition) is attractive or very attractive.’
- Reject notion of a ‘one-time password sent to them for every login’

Source: Hasham, S et al. 2016. ‘Is cybersecurity incompatible with digital convenience?’ McKinsey&Co.  
See: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608>.



- ‘Device or number recognition and omnichannel authentication (customers do not want to be treated like strangers just because they are on a different device)’
- ‘The remaining 20 percent prefer a verification phone call.’
- ‘Log-in credentials should be the same across all channels; allow for customers to log in on one channel in order to use another, eliminating duplicative authentications’

Source: Hasham, S et al. 2016. ‘Is cybersecurity incompatible with digital convenience?’ McKinsey&Co.

See: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608>.



# How to get high adoption of privacy-enhancing good security among users (Continued)

- Better visual user experience matters.
- ‘Inconsistent design, poor error messaging, clunky comms, site slowness or unavailability’ make it less appealing to the end user to accept security that will improve their privacy

Source: Hasham, S et al. 2016. ‘Is cybersecurity incompatible with digital convenience?’ McKinsey&Co.  
See: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608>.



## Privacy Policy

- A company's **privacy policy** describes how it gathers, uses, discloses, and manages a customer's information.



- Australian Information Commissioner Act
- The [Australian Information Commissioner Act 2010](#) (AIC Act) establishes the Office of the Australian Information Commissioner (OAIC).  
three primary functions:
  - **privacy** functions, conferred by the [Privacy Act 1988](#) (Privacy Act) and other laws
  - **freedom of information** functions, in particular, oversight of the operation of the [Freedom of Information Act 1982](#) (FOI Act) and review of decisions made by agencies and ministers under that Act
  - **government information policy** functions, conferred on the Australian Information Commissioner under the [Australian Information Commissioner Act 2010](#) (AIC Act).



- “Australian Privacy Principles (APPs), in schedule 1 of the *Privacy Act 1988*(Privacy Act), outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses (collectively called ‘APP entities’) must handle, use and manage personal information.
- APPs are not prescriptive, each APP entity needs to consider how the principles apply to its own situation.”



Exercise: With a partner, think about what areas of information management need to be covered by privacy principles.



- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- APP 11 — Security of personal information
- APP 12 — Access to personal information
- APP 13 — Correction of personal information



- “Separate APPs that deal with the use and disclosure of personal information for the purpose of direct marketing (APP 7), cross-border disclosure of personal information (APP 8) and the adoption, use and disclosure of government related identifiers (APP 9).”
- more stringent obligations on APP entities who handle ‘sensitive information’:
  - health (including predictive genetic information)
  - racial or ethnic origin
  - political opinions
  - membership of a political association, professional or trade association or trade union
  - religious beliefs or affiliations
  - philosophical beliefs
  - sexual orientation or practices
  - criminal record
  - biometric information that is to be used for certain purposes
  - biometric templates.



# Malicious damage to assets – in less than 60 seconds

## USB Kill Video

<https://www.youtube.com/watch?v=3hbuhFwFsDU>



## The Importance of Encryption in Email to Privacy

- “**The security of people’s communication is very important to me**”
  - Edward Snowden’s first email approach to journalist Glenn Greenwald

“The email’s .. stated purpose was to urge me to begin using PGP encryption so that ‘Cincinnatus’ could communicate things in which, he said, he was certain I would be interested.”

    - Glenn Greenwald in *‘No place to hide’*



Laura,

At this stage I can offer nothing more than my word. I am a senior government employee in the intelligence community. I hope you understand that **contacting you is extremely high risk** and you are willing to agree to the following precautions before I share more. This will not be a waste of your time.

The following sounds complex, but should only take minutes to complete **for someone technical**. I would like to confirm out of email that the keys we exchanged were not intercepted and replaced by your surveillants. Please confirm that no one has ever had **a copy of your private key** and that it uses a **strong passphrase**. Assume your adversary is capable **of one trillion** guesses per second. If the device you store the private key and enter your passphrase on has been hacked, it is trivial to decrypt our communications.

Understand that the above steps are not bullet proof, and are intended only to give us breathing room. In the end if you publish the source material, I will likely be immediately implicated. This must not deter you from releasing the information I will provide.

Thank you, and be careful.

---

Citizen Four



1. Time to complete our Role-Play Security Audit!
2. This is how you make sure someone's system is secure – hands on learning to 'cement' the concepts in your memory, (and get some practical skills in the meantime)
3. Find your buddy (same or new), choose the opposite role to last time



## 1. Patch!

- All your OS' and Applications must be up to date, fully patched.

## 2. Use strong, unique passwords:

- Use a password manager. These are a few: 1Password, LastPass, Keepass (open source password manager), Dashlane
- Or otherwise find a way to have strong, unique passwords for EACH account

## 3. Encrypt data at rest:

- Bitlocker; File Vault 2, Luks

## 4. Encrypt data in transit (i.e. avoid POTS, SMS; prefer encrypted IM like Signal, WhatsApp, Viber)

## 5. Enable mfa (multi-factor authentication); preferably using OTP-generating smartphone



1. Is your buddy's OS on phone and laptop running the latest greatest software? (fully patched)
  1. Check it now on laptop. Write down what they are running.
  2. Now check – can it be updated?
  3. Now check their phone. Not updated? Write it down.
    - running anything less than Android 7 or iOS 10.3.2, get it updated
  4. Now check their most common App – say, Office on laptops
  5. Now check the settings for updates on their phone and laptop.
  6. Who has updates to do? Make a LIST



# Encrypt data in Transit: what Encrypted message system? (Desktop & Phone)

End-to-end encrypted, audited



Signal,FB Messenger,WhatsApp,Wickr,Ricochet

E2E, but not audited



Viber, Telegram, Line, Allo,  
Wire

User-to-server encrypted



Skype, Google Hangouts

U2S → Owner



WeChat

SMS  
POTS



## More Secure Phones: Signal

### Secure messaging and voice calls.



**Free and Open Source Software, anyone can audit the code for correctness or help contribute improvements.**

**End to End Encrypted, can send txt, pics, video msgs, and talk voice over it. But not documents. Yet.**

**It uses data connection not phone. Both people need to have internet access on phone. (But no SMS or MMS Fees!)**

**It offers privacy (encryption) but NOT anonymity.**

---

**Use encryption!**



Steps:



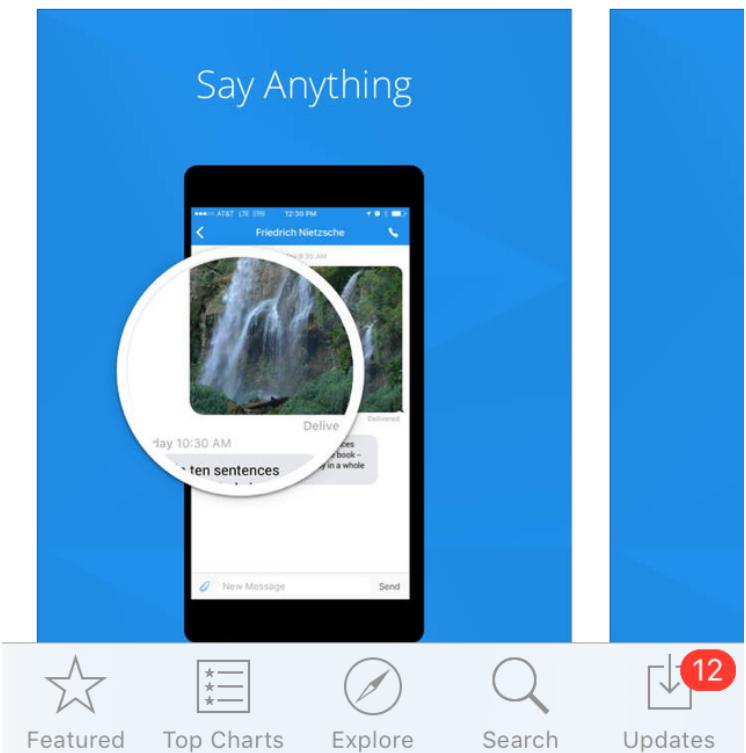
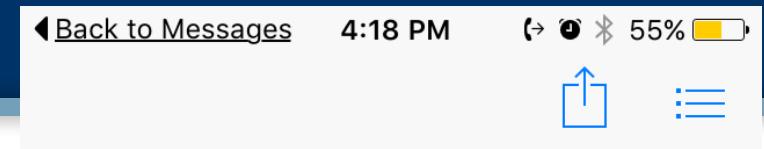
Find a buddy: share phone numbers

Open your App store in your smartphone

Search: Signal Private Messenger (by Whisper Open Systems)

Be sure you get the right App!

Download  
Open





The screenshot shows a web browser displaying the Ricochet website at <https://ricochet.im>. The page features a large blue header with the Ricochet logo and navigation links. The main content area has a white background with a dark grey sidebar on the left containing links like 'About', 'Latest changes', 'GitHub', and 'Sponsors'. The main content includes a section about anonymous messaging, download links for Windows, Mac, and Linux, and information about how it works using the Tor network.

**Ricochet**

[About](#)

[Latest changes](#)

[GitHub](#)

[Sponsors](#)

## Anonymous instant messaging for **real** privacy

Ricochet is a different approach to instant messaging that **doesn't trust anyone** in protecting your privacy.

- *Llminate metadata.* Nobody knows who you are, who you talk to, or what you say.
- *Stay anonymous.* Share what you want, without sharing your identity and location.
- *Nobody in the middle.* There are no servers to monitor, censor, or hack.
- *Safe by default.* Security isn't secure until it's automatic and easy to use.

### Get started

The latest version is **1.1.2** (February 15, 2016). You can also [build from source](#).

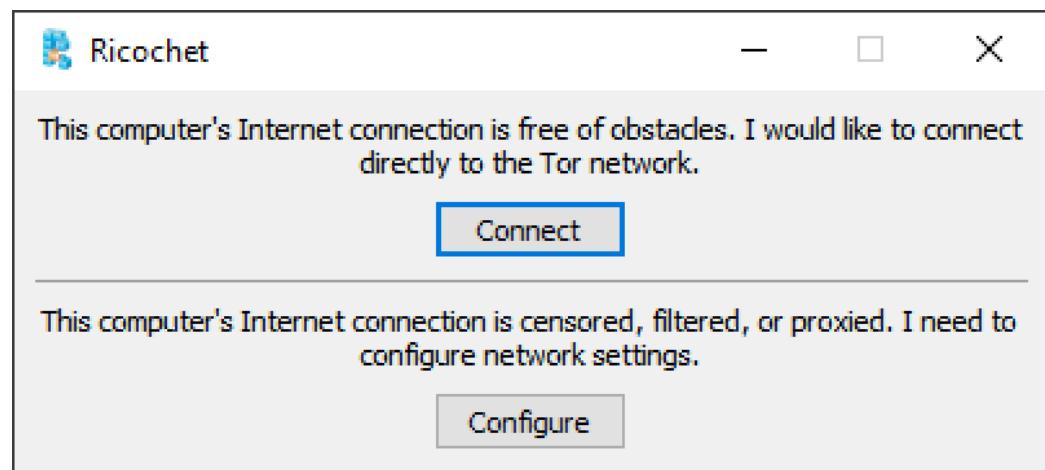
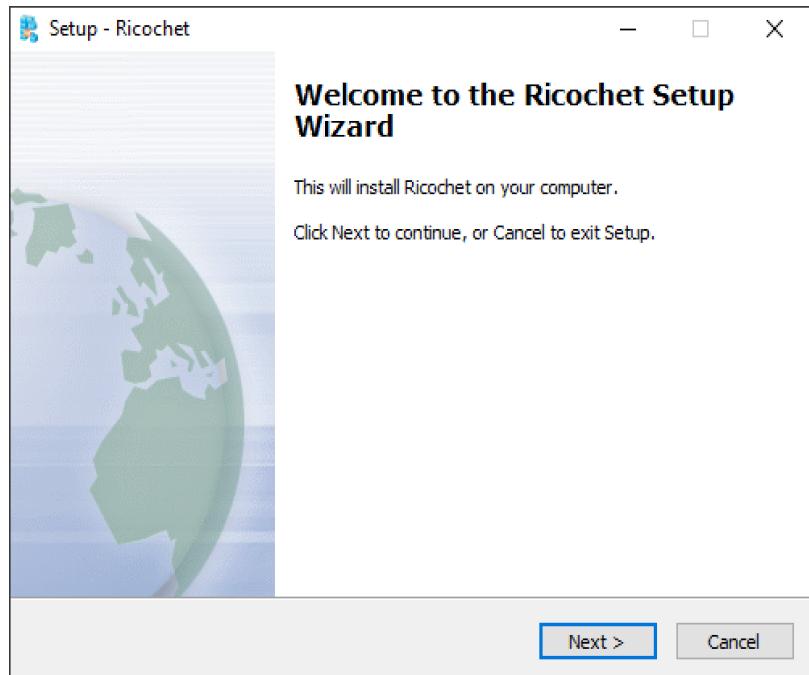
#### How it works

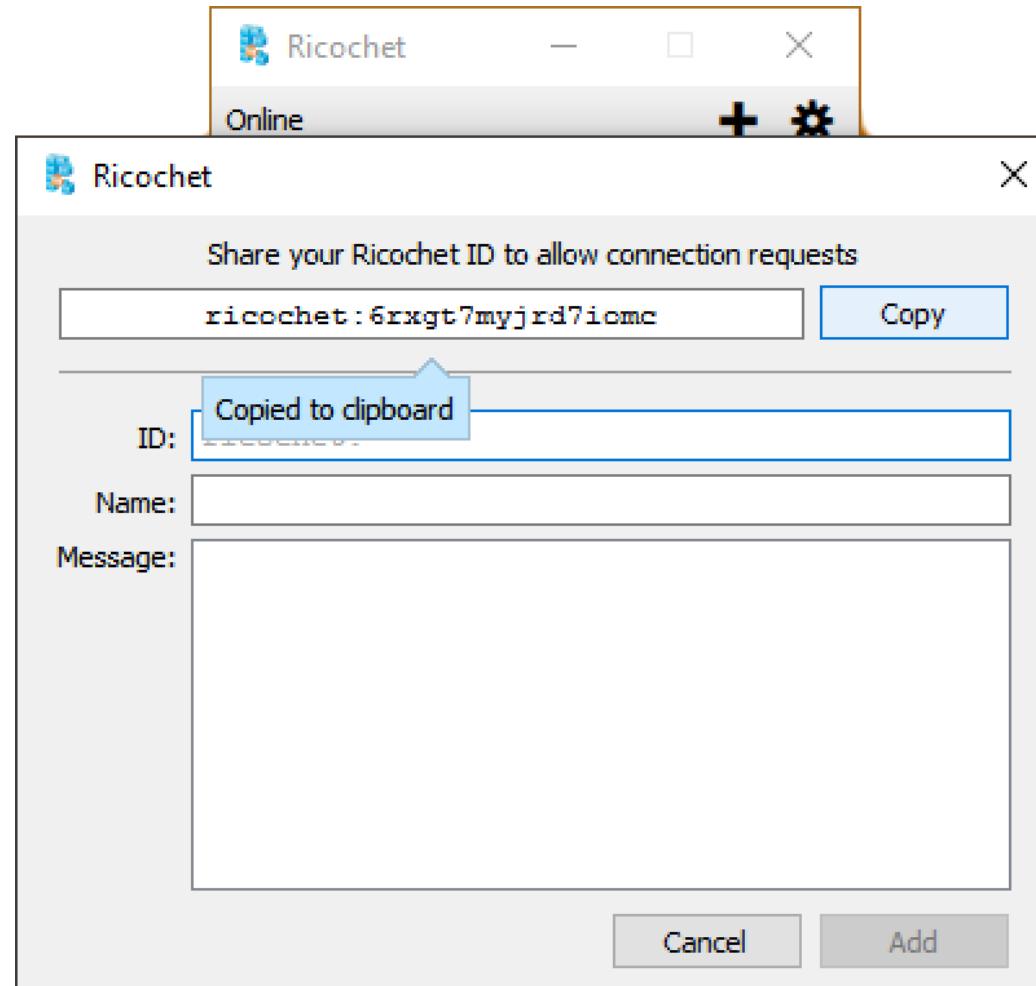
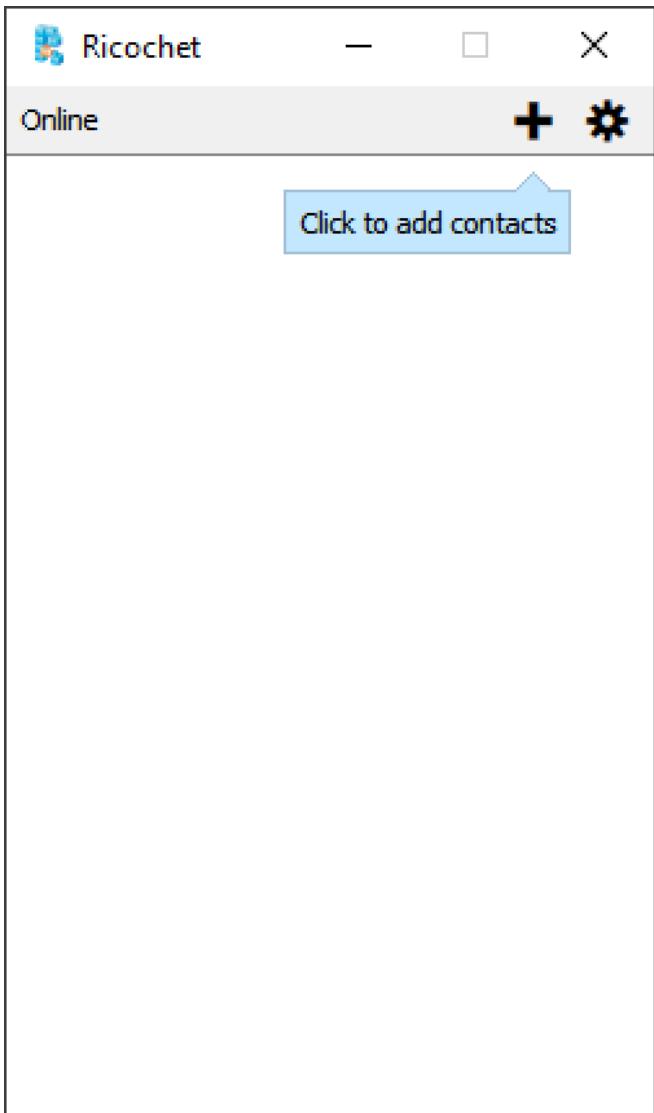
Ricochet uses the [Tor network](#) to reach your contacts without relying on messaging servers. It creates a [hidden service](#), which is used to rendezvous with your contacts without revealing your location or IP address.

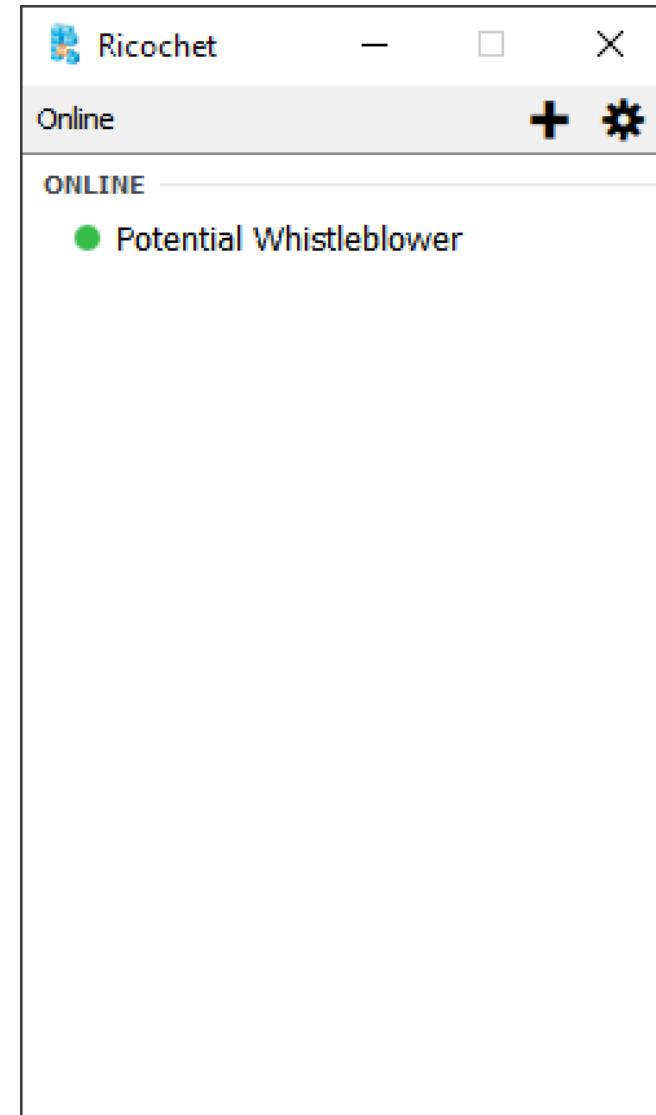
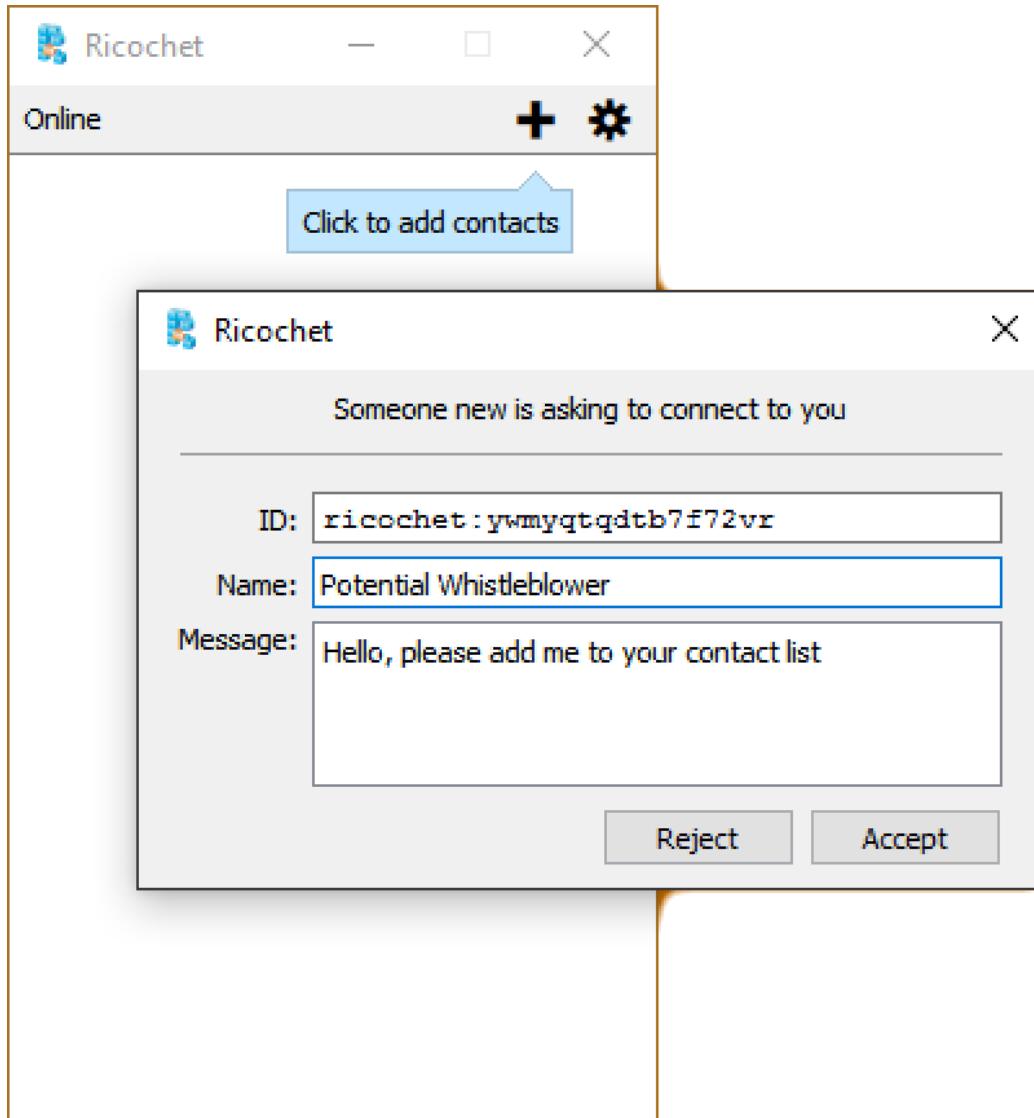
Instead of a username, you get a unique address that looks like [ricochet:rs7ce36jsj24ogfw](#). Other Ricochet users can use this address to send a *contact request* - asking to be added to your contacts list.

You can see when your contacts are online, and send them messages (and soon, files!). Your list of contacts is only known to your computer - never exposed to servers or network traffic monitoring.

Everything is encrypted *end-to-end*, so only the intended recipient can decrypt it, and anonymized, so nobody









Ricochet

Online + ⚙

ONLINE

● Potential Whistleblower

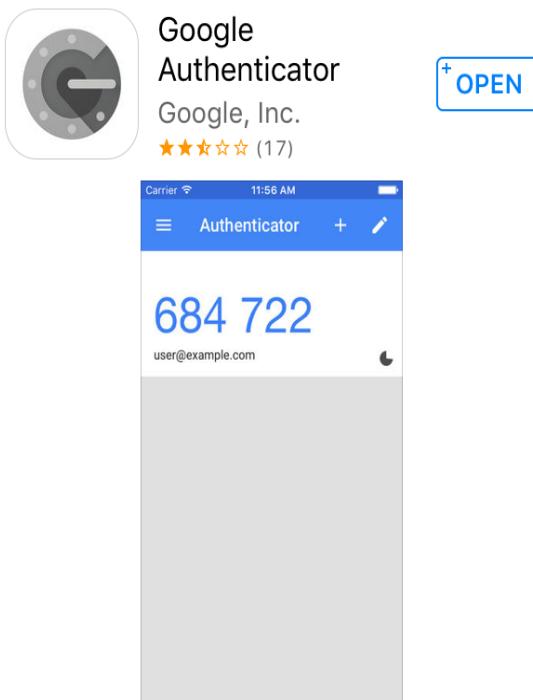
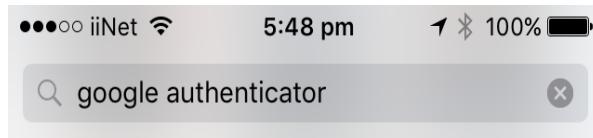
Potential Whistleblower

● Potential Whistleblower

28/06/2016 2:21 PM

Hello, I have something interesting for you

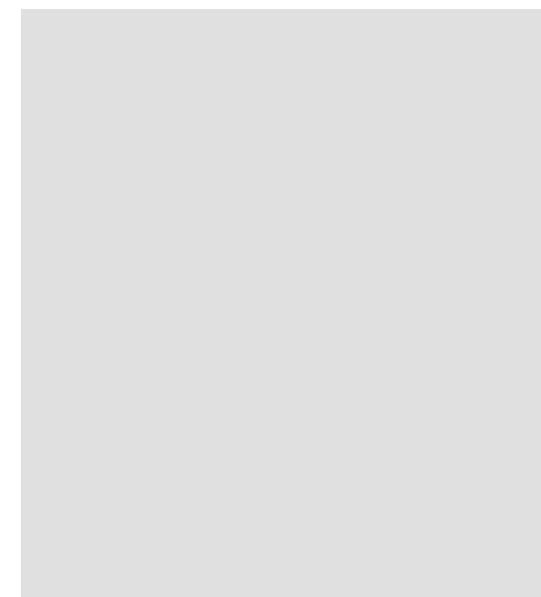
Cool, thanks for contacting me



Facebook

103 637

lois.lane





# 2 Factor Authentication - Gmail



The screenshot shows the Google My Account interface. At the top, there's a blurred header bar with the URL "https://myaccount.google.com/2stepauth". Below it, the Google logo and "My Account" are visible. On the right side, there's a profile picture and icons for Gmail, Google Photos, Google Sheets, and YouTube. The main content area has a heading "Control, protect and secure your account." followed by a subtext: "My Account gives you quick access to settings and tools that let you configure your data, protect your privacy, and work better for you." Below this, two main sections are shown: "Sign-in & security" (with a lock icon) and "Personal info & privacy" (with a person icon). Each section has a descriptive subtitle underneath.

Welcome, Emma Bellis

Control, protect and secure your account.

My Account gives you quick access to settings and tools that let you configure your data, protect your privacy, and work better for you.

[Sign-in & security](#)

[Personal info & privacy](#)



The screenshot shows a web browser window with a blue header bar. Below it, a white page displays a message about password & sign-in methods. A large blue button labeled "Change settings" is visible. On the left, there's a sidebar with options like "Account & privacy", "Security", "Sign-in methods", and "Two-step verification". The main content area has a heading "2-Step Verification" with the status "On since: 19 June 2016". Below this, there are sections for "App passwords" and "More".

password & sign-in methods

Your password protects your account. You can also add a second layer of protection with a code sent to your phone, which works as a simple way to verify who you're talking to when you log in. This adds an extra layer of security to your account, so we highly recommend you turn on 2-Step Verification.

Change settings

2-Step Verification

On since: 19 June 2016

App passwords

More



The screenshot shows a web-based interface for managing two-factor authentication (2FA) for a Gmail account. At the top, there's a blue header bar with the text "2fa - Gmail". Below this, a banner displays a QR code and the text "QR code verification is valid until 19 June 2016" with a "Rescan QR" button.

The main content area is titled "Your second step" and includes a note: "After verifying your permanent phone you'll be asked for a second verification step." It features a "Next step" button.

A section titled "Would you like to receive verification codes?" contains a question "Can I change which app or device I receive verification codes from?" and a "Read more" link.

Below this, a card lists an existing 2FA method:

- Authenticator app (Default)** (with a help icon)
- Type: Authenticator on iPhone
- Added: 19 June 2016
- Change Phone (button)

At the bottom, there's a "Delete or Edit message" button.



### Set up alternative second step

Set up at least one backup option so that you can sign in even if your other second steps aren't available.



#### Backup codes

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.

[SET UP](#)



#### Google prompt

Get a Google prompt on your phone and just tap **Yes** to sign in.

[ADD PHONE](#)



#### Security Key

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. [Learn more](#)

[ADD SECURITY KEY](#)



# 2fa - Facebook

Your Pages:

Blueprint for Free Spe... [2]

Create Page

Manage Pages

Create Group

New Groups 4

Create Ads

Advertising on Facebook

Activity Log

News Feed Preferences

**Settings**

Log Out



A screenshot of a Facebook settings page titled "Security and Login". The left sidebar shows a navigation menu with the following items:

- General
- Security and Login** (selected)
- Privacy
- Timeline and Tagging
- Blocking
- Language
- Notifications
- Mobile
- Public Posts
- Apps
- Ads
- Payments
- Support Inbox
- Videos

The main content area displays the "Security and Login" settings. It includes sections for "Recent devices" (Windows PC - Alphington, VIC, Australia) and "Recent mobile devices" (iPhone 6s - Alphington, VIC, Australia). There is also a "See More" link at the bottom.



A screenshot of a Facebook two-factor authentication settings page. The page has a light gray background with a dark blue header bar at the top. In the center, there's a white rectangular box containing several sections of text and icons.

**Use two-factor authentication**

**On** • Log in with a code from your phone as well as a password Close

---

Two-factor authentication is on. Turn Off

Add an extra layer of security to prevent other people from logging into your account. [Learn More](#)

---

**Text Message (SMS) · Add Phone**

Use your phone as an extra layer of security to keep other people from logging into your account.

[Add phone](#) [Remove phone](#)

---

**</> Code Generator · Disable**

You can use Code Generator in your Facebook mobile app to reset your password or to generate login codes. Set up a [third party app](#) to



A screenshot of a web browser window. At the top, there are several tabs and icons. Below the tabs, a sidebar on the left lists "Two-factor authentication" and "Use Two-Factor authentication". A central modal dialog box is open, titled "Set Up a Third Party App to Generate Codes". Inside the dialog, there is a message: "To get a third party app working, either scan the QR code below or type the secret key into the app." Below the message is a QR code. At the bottom of the dialog, there is a green button labeled "Get started >>>".



[Close](#)

# 2fa

# Facebook



## Use two-factor authentication

[On](#) • Log in using a code from your phone as well as a password

Two-factor authentication is on.

[Turn off](#)

Add an extra layer of security to prevent other people from logging in to your account. [Learn more](#)



### [Text message \(SMS\)](#) · [Add phone number](#)

Use your phone as an extra layer of security to keep other people from logging in to your account.

**0419 879 350**

[Enabled](#) · [Disable](#)



### [Security keys](#) · [Add key](#)

Use a Universal 2nd Factor (U2F) security key to log in via USB or NFC.



### [Code generator](#) · [Disable](#)

You can use Code Generator in your Facebook mobile app to reset your password or generate login codes. Set up a [third-party app](#) to generate codes.



### [Recovery codes](#) · [Get codes](#)

Use these codes when you don't have your phone with you, such as when you're travelling.



### [App passwords](#) · [Generate](#)

Get a unique, one-off password for apps that don't support two-factor authentication (e.g. Xbox, Spotify) [Learn more](#)



### [Authorised logins](#) · [Close](#)

Review a list of devices on which you won't have to use a login code



### Advanced



#### Encrypted notification emails

Add extra security to notification emails from Facebook (only you can decrypt these emails)

[Close](#)

#### Your OpenPGP public key

Enter your OpenPGP public key here:

Enter a PGP public key

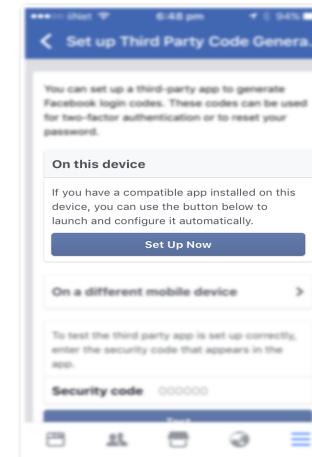
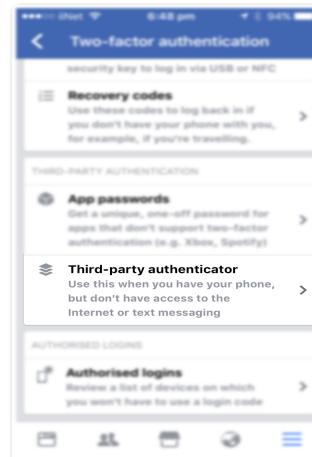
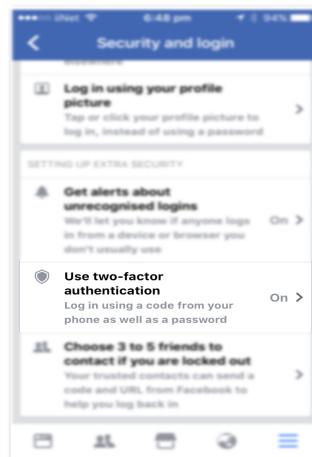
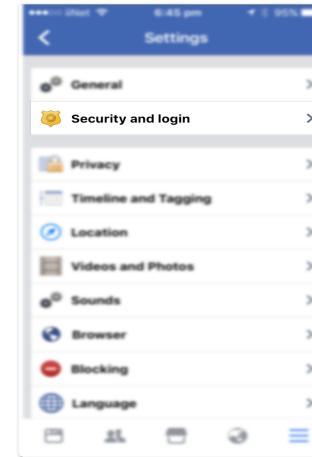
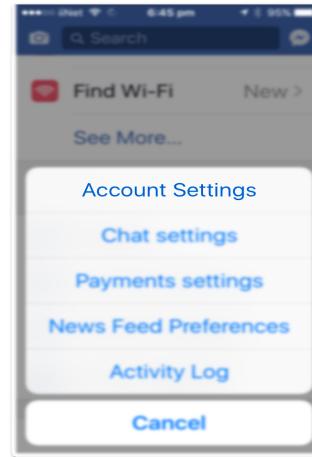
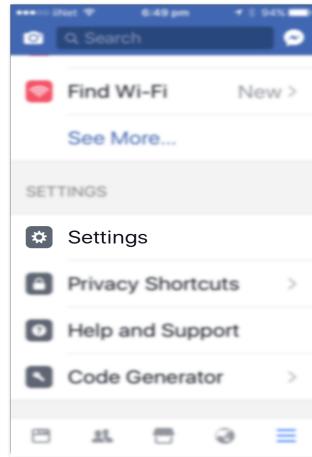
Use this public key to encrypt notification emails that Facebook sends you? [\[?\]](#)

If you wish to share your public key, you can change who can see it in your profile's [Contact and basic info about page](#).

You can download Facebook's public key [here](#).

[Save Changes](#)

# 2fa – Facebook setup on Phones





A screenshot of a Twitter profile page for a user named Emma Baillie (@EmmaBaillie). The profile picture is a blue icon. The stats show 11 tweets, 134 followers, and 22 following. Below the stats, there's a section titled "Who to follow" with three suggestions: "Followed by James Tap and others" (Palliative Care QLD), "Followed by St. John's Church and" (Sik Huang), and "Followed by Pamela Carr (Government)". There's also a link to "Find people you know". On the right, there's a sidebar for "Emma Baillie" with options: Profile, Lists, Moments, Twitter Ads, Analytics, Settings and privacy (which is highlighted in blue), Help Center, Keyboard shortcuts, and Log out. The main feed shows a tweet from "Hootsuite" (@hootsuite) about social media tips, and another from "March" (@marchgroup) about personal values.



The screenshot shows the Twitter account settings page for a user named Emma Baillie (@EmmaOBaillie). The main content area is titled "Account" and displays basic account information: Username (EmmaOBaillie), Email (emmaobaille@mebigapple.net.au), Language (English), and Time zone (EDT-0700 Pacific Time (US)). Below this, a "Security" section is highlighted with a white background. It contains a "Login verification" section with a checked checkbox for "Verify login requests". A note explains that after logging in, Twitter will send an SMS message with a code to +61488584018. There are two buttons: "Setup a code generator app" and "Get Backup Code". The "Get Backup Code" button is described as saving a backup code for future logins if the device is lost. At the bottom of the "Security" section, there is a "Generate app password" button for temporary logins to third-party apps. A "Password reset" link is also present. The footer of the page includes links for "About", "Help Center", "Terms", "Privacy policy", "Cookies", "Autofill", "Brand", "Blog", "Status", "Apps", "Jobs", "Advertiser", "Business", and "Developers".



•••oo iiNet ⌘ 3:00 pm 1 ⌘ 72% 🔋

**Emma Baillie**  
@EmmaOBaillie

114 Following 22 Followers

- Profile
- Lists
- Moments

---

Settings and privacy

Help Center

...

...

•••oo iiNet ⌘ 3:01 pm 1 ⌘ 72% 🔋

**Settings and privacy**

@EmmaOBaillie

- Account
- Privacy and safety
- Notifications
- Content preferences

General

- Display and sound
- Data usage
- Accessibility
- About Twitter

...

...

•••oo iiNet ⌘ 3:01 pm 1 ⌘ 72% 🔋

**Account**  
@EmmaOBaillie

**Login and security**

- Username @EmmaOBaillie
- Phone +61 488 584 018
- Email ebaillie@netspace.net.au
- Security

**Data and permissions**

- Your Twitter data

Log out

...

...



••••• iiNet 3:01 pm 72%

- Security**  
@EmmaOBaillie
- Login verification 
  - Login code generator >
  - Backup code >

Temporary password >

••••• iiNet 3:02 pm 72%

- Login code generator**  
@EmmaOBaillie
- Enter this code to complete login to your Twitter account.

545 096 C

This code will update every 30 seconds.

You can also use a third party authenticator app to generate login verification codes. [Learn more](#)

••••• iiNet 3:13 pm 69%

Cancel

We've texted you a login verification code.

Please check your phone with number ending in **18** for a six-digit code and enter it in the box below to log in.

You may also generate a code using the [Login code generator](#) in the Twitter app on your iOS / Android device. This works even when your device is **offline**.

Enter code

Submit

You can also [use a saved backup code](#) to log in.

Need help? Please contact [Twitter Support](#).





1. Tweak your IM settings
  - WhatsApp
2. Think paper printouts are safer? Think again
3. Turn off Bluetooth when you're not using it!
4. Browse with More Privacy



## Whatsapp – removing cloud backup

•••oo iiNet 2:46 pm 75%

Settings

Emma Hey there! I am u... >

Starred Messages >

WhatsApp Web/Desktop >

Account >

Chats >

Notifications >

Status Calls Camera Chats Settings

•••oo iiNet 4:53 pm 60%

Settings Chats <

Chat Wallpaper >

Save to Camera Roll

Automatically save photos and videos you receive to your iPhone's Camera Roll.

Chat Backup >

[Archive All Chats](#)

[Clear All Chats](#)

Status Calls Camera Chats Settings

•••oo iiNet 4:54 pm 60%

Chats Chat Backup <

Last Backup: Never Total Size: -

Back up your chat history and media to iCloud so if you lose your iPhone or switch to a new one, your chat history is safe. You can restore your chat history and media when you reinstall WhatsApp. Media and messages you back up are not protected by WhatsApp end-to-end encryption while in iCloud.

[Back Up Now](#)

Auto Backup Off >



## Whatsapp – Key Verification like Signal

•••oo iiNet 2:50 pm 74% 🔋

Suelette Dreyfus last seen today at 2:12 pm

Today

🔒 Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

+ |

I Yes I'm

Q W E R T Y U I O P  
A S D F G H J K L  
Z X C V B N M   
 123 space return

•••oo iiNet 2:51 pm 73% 🔋

Suelette Contact Info Edit

Suelette Dreyfus +61 419 879 350

Media, Links and D... None >

Starred Messages None >

Mute No >

Custom... Default (Note) >

Save Media to C... Default >

Encryption

Messages to this chat and calls are secured with end-to-end encryption. Tap to verify.

•••oo iiNet 2:52 pm 73% 🔋

Verify Security Code You, Suelette

38999 30091 38982 77599  
62249 56887 77978 48721  
02204 93396 65223 40920

Scan the code on your contact's phone, or ask them to scan your code, to verify that the messages and calls with them are end-to-end encrypted. You can also compare the number above to verify. This is optional. [Learn more.](#)

Scan Code



••ooo iiNet 2:46 pm 75% 🔋

## Settings

Emma Hey there! I am u... >

Starred Messages >

WhatsApp Web/Desktop >

Account >

Chats >

Notifications >

Status Calls Camera Chats Settings

••ooo iiNet 2:46 pm 75% 🔋

◀ Settings Account

Privacy >

Security >

Two-Step Verification >

Change Number >

Delete My Account >

Status Calls Camera Chats Settings

••ooo iiNet 2:47 pm 75% 🔋

◀ Account Security

Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.

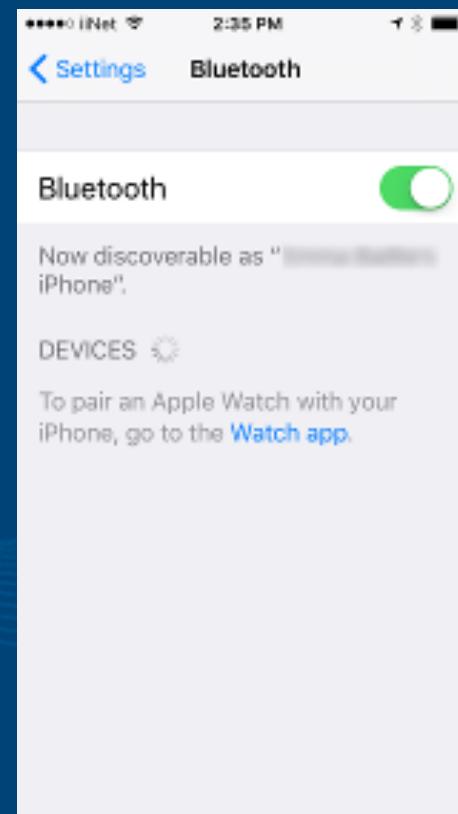
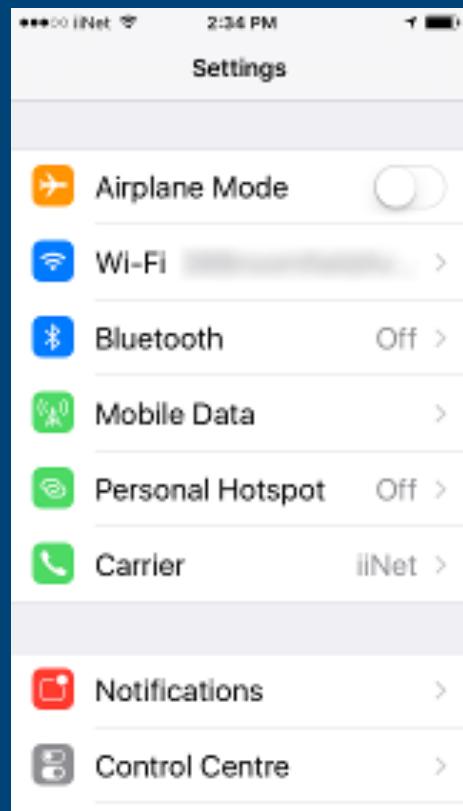
[Learn more about WhatsApp security.](#)

Show Security Notifications

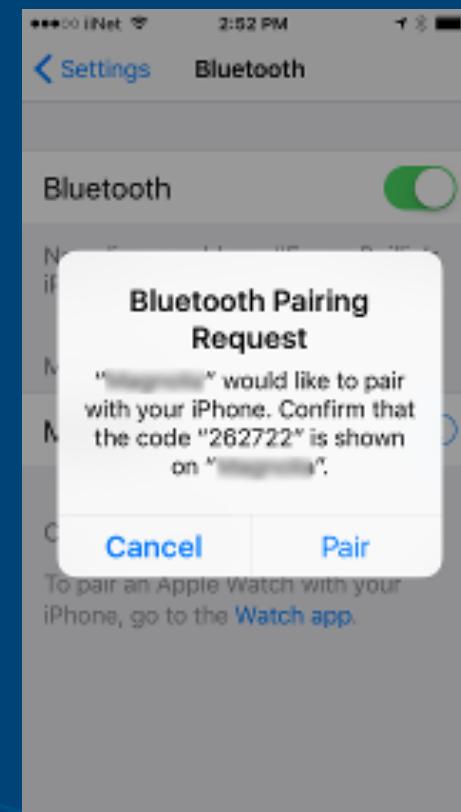
Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.

Status Calls Camera Chats Settings

## Bonus Track: Turn off Bluetooth



# Bluetooth in your phone's settings





IMENT PAGES TEXT Zoom

p. 1

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

DIRNSA [REDACTED]

National Security Agency

**Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [REDACTED] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)**

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

**SUMMARY (U)**

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [REDACTED] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance

[REDACTED]

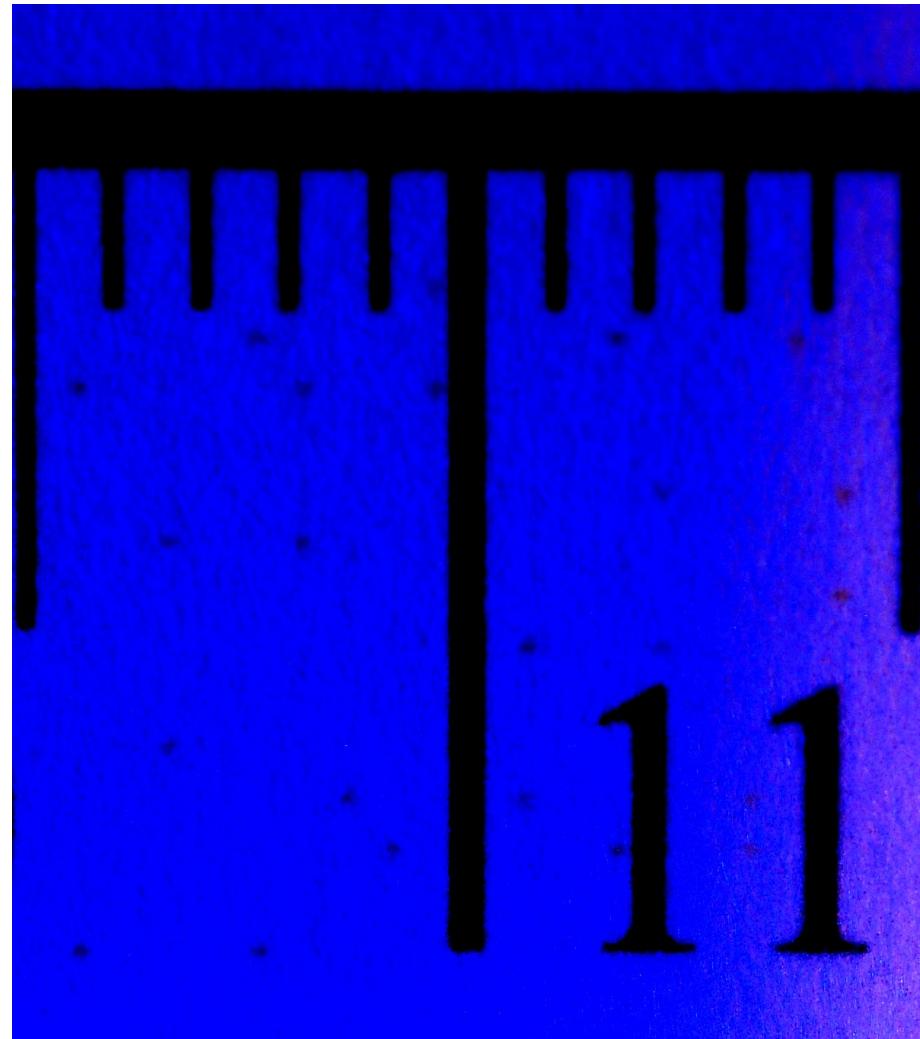
Declassify On: 20420505

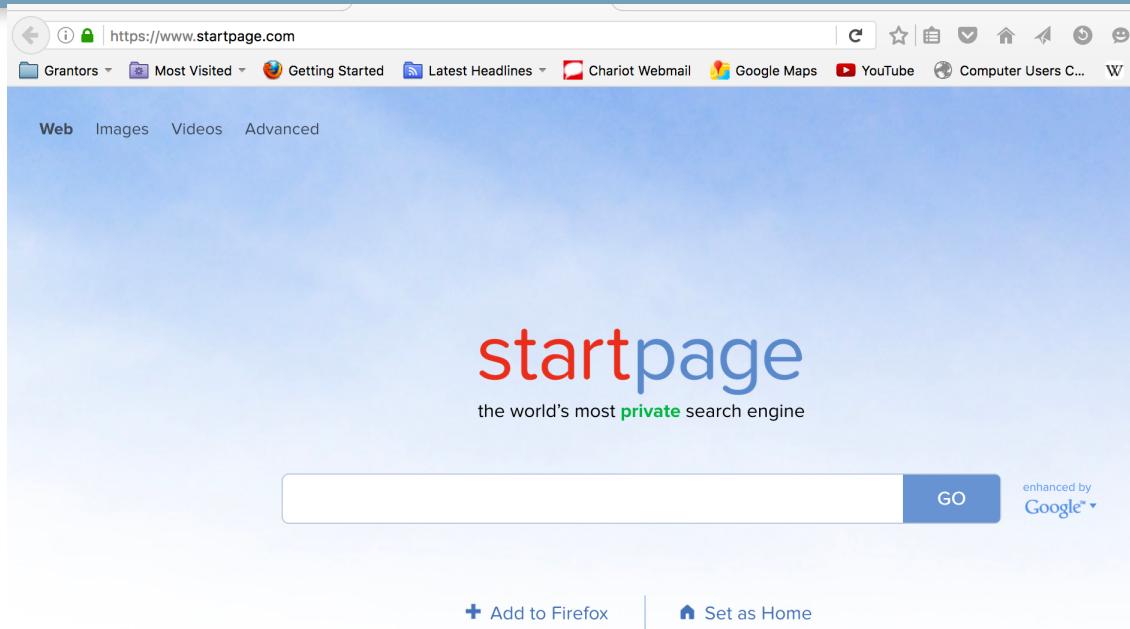
Page 1





- Secret information – yellow dots which can be seen under blue light or with digital manipulation - encoded in the documents when they were printed may have allowed her identity to be quickly exposed.





Set it as your  
default search  
engine in your  
browser

### Option 1 <https://startpage.com>

Similar quality search results to Google. Your searches are proxied to Google – it looks like Startpage is making the search. No metadata from you is kept.

Reasonable anonymity (not perfect) unless searching something unique to you (great-grandfather's name etc)



The screenshot shows a search interface with a magnifying glass icon and a red circular profile picture. The search term 'duck' is entered in the search bar. Below the search bar are navigation links: Web, Images, Videos, Meanings, **About**, Recipes, and Definition. The main search results section features the DuckDuckGo logo (a white duck wearing a bow tie inside a red circle) and the text 'DuckDuckGo'. A detailed description follows: 'DuckDuckGo is an Internet search engine that emphasizes protecting searchers' privacy and avoiding the filter bubble of personalized search results. DuckDuckGo distinguishes itself from other search engines by not profiling its users and by de...'. Below this are links to 'Show More', 'More at Wikipedia', and the website 'duckduckgo.com'. To the right of the main results are vertical tabs for 'Slogans', 'Type', 'Owner', 'Creator', and 'Launch Date'. Below the main results, there is another section for 'DuckDuckGo' with a brief description and a link to 'duckduckgo.com'.

Set it as your default search engine in your browser

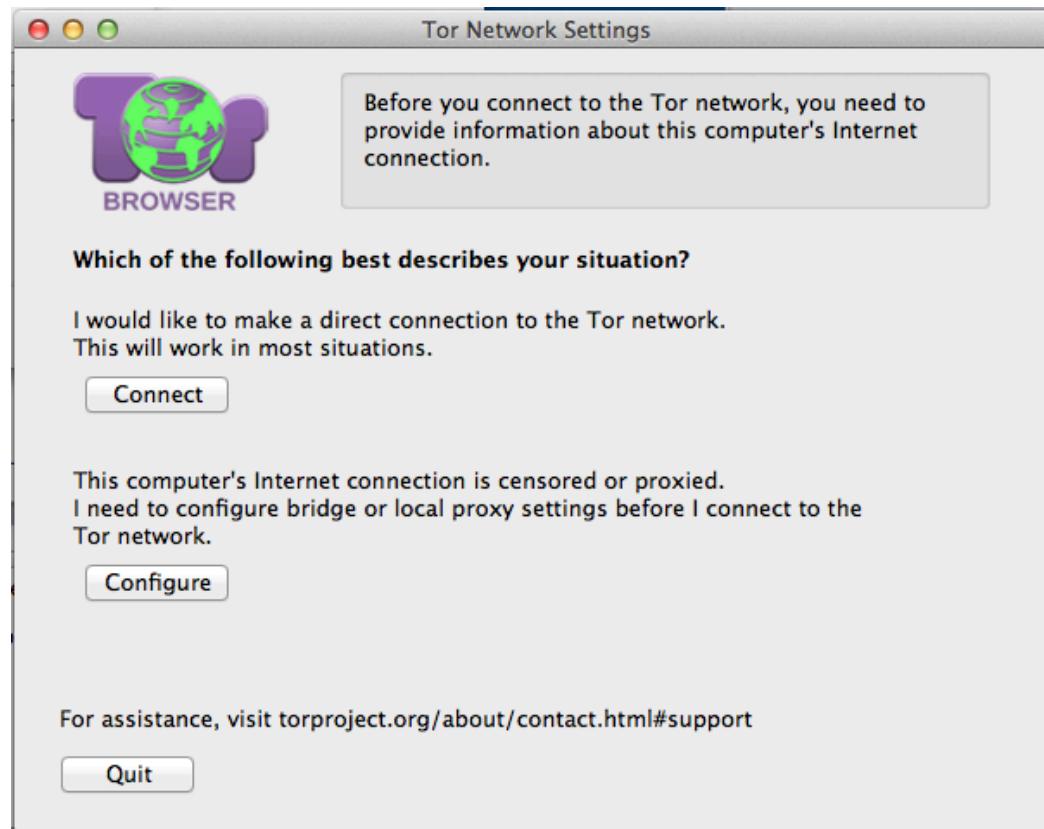
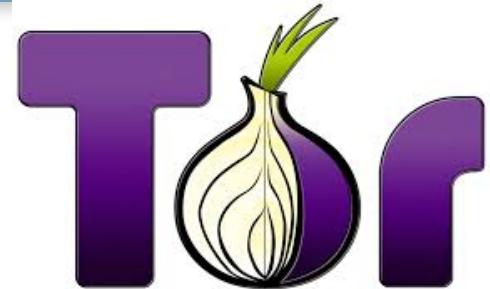
## Option 2 <https://duckduckgo.com>

Will turn up different search results than Google, because they index the web themselves. They don't send your request onto anyone.

Their privacy policy says: metadata and searches are kept.



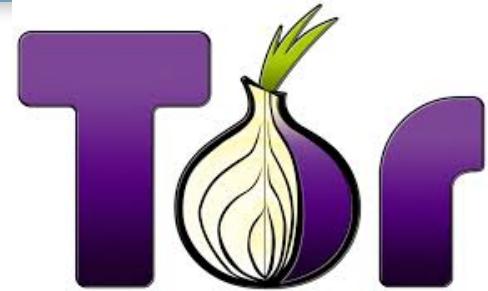
<https://www.torproject.org/>





<https://www.torproject.org/>

<https://check.torproject.org/>



### TOR Principles

- Use the TOR Browser
- Don't torrent over TOR
- Don't open downloaded documents when online



## How Unique is your browser?

<https://panopticlick.eff.org/>

Your browser fingerprint **appears to be unique** among the 129,323 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 16.98 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here](#).

Test	Result
Is your browser blocking tracking ads?	⚠ partial protection
Is your browser blocking invisible trackers?	⚠ partial protection
Does your browser unblock 3rd parties that promise to honor <a href="#">Do Not Track</a> ?	✗ no
Does your browser protect from <a href="#">fingerprinting</a> ?	✗ your browser has a unique fingerprint

Class hands on: run it now – share the answer



With special thanks to the following for material that has been adapted and incorporated:

TROPE: Teachers' Resources for Online Privacy Education, which is supported by a grant from the National Science Foundation: DGE-1419319, with additional support from NSF grants EEC-1405547 and CCF-0424422 and from IISME.

Any opinions, findings, and conclusions or recommendations are those of the originators and do not necessarily reflect the views of the National Science Foundation.

Licensed by the International Computer Science Institute under a Creative Commons Attribution 4.0 License (CC-BY)

Thoughtworks workshop training CryptoParty Melbourne trainers