

# Privacy, security and some basic e-sleuthing

Peter Aldhous

[peter@peteraldhous.com](mailto:peter@peteraldhous.com)

Twitter: [@paldhous](https://twitter.com/paldhous)

# Don't assume your emails, phone calls, web surfing and searches are private ...

MEDIA & ADVERTISING

## *Head of The A.P. Criticizes Seizure of Phone Records*

By RAVI SOMAIYA    MAY 19, 2013

The head of The Associated Press said on Sunday that the Obama administration's secret seizure of two months of its phone records, revealed this month, was "unconstitutional," and had already diminished journalists' capacity to report on the government.

The Justice Department has been widely criticized for the seizure, which covered 20 A.P. telephone lines, including its offices and the home phones and cellphones of journalists. The records were obtained without notice, directly from the phone company.

Thanks to this guy, I don't need to tell you that...

**theguardian**

News | US | World | Sports | Comment | Culture | Business | Money | Environment | Science

News > World news > The NSA files

## Edward Snowden, NSA files source: 'If they want to get you, in time they will'

Source for the Guardian's [NSA files](#) on why he carried out the biggest intelligence leak in a generation – and what comes next

**Ewen MacAskill**  
Follow @ewenmacaskill Follow @guardian  
The Guardian, Sunday 9 June 2013

Share 116  
Tweet 17  
+1 2k  
in Share 1  
Email

Article history

### The NSA Files: Decoded



# **Let's not get paranoid ...**

## **Consider the threat – which is usually minimal**

- What do I need to keep secret? (e.g. content of communication, source identities, files)
- Who do I need to keep it secret from? (the "adversary," e.g. government, source's employer, competing news orgs)
- What can they do to find out? (consider technical, legal, and social means)
- What happens if they do find out? (this is the risk, and will tell you how serious you need to be)

[Exercises](#) and [lecture](#) on threat modeling for journalists from [Jonathan Stray](#)

**But sometimes we may need to cover our tracks**

# Web surfing

Every time you visit a website you reveal:

- **Operating system**
- **Regional and language settings**
- **Connection's "host name"**

May allow people to guess your name, email address and so on

- **IP address**

May identify where you work. Even surfing from home, IP addresses may identify you – for example they can appear next to messages left in online communities, and can be Googled.

- **Referring page**

Reveals the link from which you clicked, or your search terms, if you are coming from a search engine.

Websites can also deposit tracking "cookies" on your machine

**Check what information will be displayed to any website you visit:**

<http://www.ip-secrets.com/>  
<http://whatismyipaddress.com/>  
<http://anonymouse.org/cgi-bin/anon-snoop.cgi>

**To hide your IP address from a website:**

**Cover your tracks with an anonymous proxy server**

<http://anonymouse.org/anonwww.html>  
[http://www.guardster.com/subscription/proxy\\_free.php](http://www.guardster.com/subscription/proxy_free.php)

(Free for most surfing but may need to upgrade to paid service to access encrypted links anonymously)

**(Or use coffee-shop wi-fi)**

# **For a more systematic approach:**

**Install software to anonymize your web browsing:**

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

(See <https://www.torproject.org/download/download.html.en#warning> to learn how to alter your browsing behavior to use Tor effectively)

**<https://www.privateinternetaccess.com/>**  
**<https://www.anonymizer.com/>**

(See [this article](#) for pros and cons of Tor vs VPN services like PIA and Anonymizer)

**For private web searching:**

**<https://www.ixquick.com/>**

**<https://startpage.com/eng/protect-privacy.html>**

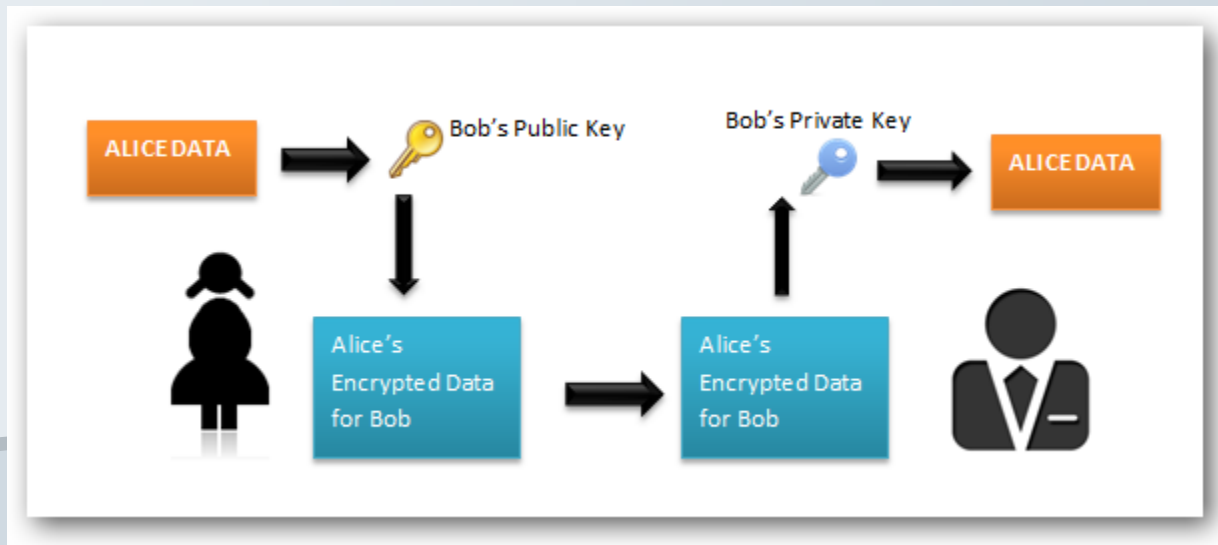
(See [here](#) for their policies)

# Email

**Use two-factor authentication for webmail services**

**Encrypt emails that you need to keep between you and a confidential source!**

**The basics, from [here](#):**





# Encrypted email options

## Enigmail for Thunderbird

<https://emailselfdefense.fsf.org/en/>

<https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages>

## Coming soon, End-to-End for Gmail

<http://googleonlinesecurity.blogspot.com/2014/12/an-update-to-end-to-end.html>

## Encrypted email service:

<http://www.hushmail.com/>

(See <http://www.hushmail.com/about/technology/security/> for details of service/policies)

# More encryption

## Encrypted chat

<https://crypto.cat/>  
<https://adium.im/>

## Encrypt files

<http://support.gpgtools.org/kb/gpgservices-faq/how-to-encrypt-and-sign-text-or-files-with-gpgservices>

(uses [GPG tools](#), for Mac, see [here](#) and [here](#) for other tools for Mac, Windows and Linux)

## Encrypt your laptop's hard drive

<https://firstlook.org/theintercept/2015/04/27/encrypting-laptop-like-mean/>

[Here](#) is a good overview of encryption in the context of journalism

# Email

## Tracing emails:

Paste email headers here:

<http://whatismyipaddress.com/trace-email>

[http://www.ip-adress.com/trace\\_email/](http://www.ip-adress.com/trace_email/)

Lesson: throwaway Gmail accounts provide some anonymity

# Phone

## Caller ID

- \*67 blocks caller ID
- You can spoof caller ID with <http://www.spoofcard.com/>

## Cellphones

- GPS enabled phones are personal tracking devices
- For private/anonymous conversations, use prepaid cellphones, paid for with cash, switch off and remove battery when not in use

# Removing files from your computer

Deleting files does not destroy them, so to remove traces you need to overwrite them:

**Windows:** <http://eraser.heidi.ie/>

**Mac:** see [this article](#)

## Putting it all together

[This article](#) reveals the exhaustive steps a confidential source would need to take to be sure their identity is secure

# Who is behind a website?

## Whois

<http://www.easywhois.com>

<http://whois.domaintools.com/>

## Whois history

<http://www.domaintools.com/research/whois-history/>

# What other websites are hosted at the same IP address?

[http://www.ip-adress.com/reverse\\_ip/](http://www.ip-adress.com/reverse_ip/)

<http://www.linkvender.com/seo-tools/domains-from-ip.html>

# Retrieve old/defunct websites and pages

## Google Cache

Do a normal Google search, scroll over the downward facing triangle next to the url and select the Cached link.

## Wayback Machine

<http://www.archive.org/web/web.php>

## CyberCemetery

<http://govinfo.library.unt.edu/default.htm>

Archive of retired government web pages; look for missing reports etc

## Monitor websites for changes

<http://www.changedetection.com/>

**Or Firefox add-ons:**

<https://addons.mozilla.org/en-us/firefox/addon/alertbox/>

<https://addons.mozilla.org/en-us/firefox/addon/sitedelta/>

**As we've already noted:** Websites are likely to change if their owners realize that information on the site is incriminating. So save web pages that are key to an investigation!



# **Social media searches**

**Paul Myers' social network search tool**

**<http://www.google.com/cse/home?cx=016007582557612459539:wxiudovjrjc>**

**Whos Talkin**

**<http://www.whostalkin.com/>**

**Icerocket**

**<http://www.icerocket.com/>**

## **Other resources**

**Compilation of search resources for legal professionals**

**<http://www.llrx.com/features/ciguide.htm>**

**World phone directories**

**<http://www.infobel.com/en/world/index.aspx>**

# Privacy, security and some basic e-sleuthing

Peter Aldhous

[peter@peteraldhous.com](mailto:peter@peteraldhous.com)

Twitter: [@paldhous](https://twitter.com/paldhous)