Hints and Tips for Whistleblowers

Technical Hints and Tips for protecting the anonymity of sources for
Whistleblowers, Investigative Journalists,
Campaign Activists and Political Bloggers etc.
by **Spy Blog**
http://ht4w.co.uk

http://r3lb3r3an7uj7bos.onion/
https://r3lb3r3an7uj7bos.tor2web.org/

Introduction

By
wtwu
on June 11, 2011 10:00 PM | Permalink | Comments (0)

Over the years, Spy Blog has been the willing and sometimes unwilling, recipient of various confidential secrets, some of which we have been asked to pass on anonymously to the mainstream media or to the appropriate government authorities.

This mini-blog splits up, and ~~slightly~~ greatly expands, what had become a rather long and cumbersome single Spy Blog posting Home Office whistleblowers - hints and tips, originally published in May 2006.

This was prompted by the whistleblower leaks to the media, and by appeals for further such leaks by political bloggers, regarding the appalling state of the Home Office, especially the scandals over Prisons and the inept non-deportation of foreign prisoners etc.

This lead to the resignation of one Labour Home Secretary Charles Clarke and the description of the Home Office, by his equally incompetent and repressive Labour successor John Reid as being "dysfunctional and not fit for purpose".

The later, scandalous arrest and searches of the then Conservative front bench immigration spokesman (now a Home Office Government Minister) Damian Green MP's home, constituency and Parliamentary offices, and the Home Office whistleblower Christopher Galley, in 2008 and their subsequent vindication in 2009, show how the civil service bureaucrats and the Labour politicians currently power, like to spuriously invoke "national security", when they are really trying to suppress purely political scandals, for which they are to blame, from being made public.

All well and good, but many of the whistleblowers, investigative journalists, bloggers and activists etc. are **not very skilled at protecting the anonymity of their whistleblower or journalistic sources**, especially when using today's computer and mobile phone technology.

Even where a whistleblower knows that they will eventually have to go public, there is often a crucial time period during which they want or need to protect their anonymity.

It is scandalous that we should even need to think about the same sort of techniques which are needed by people living under repressive dictatorships, when we live in a supposed "liberal western democracy" here in the United Kingdom, but unfortunately these internationally applicable practical hints and tips, are becoming increasingly necessary.

If you are leaking information to the press or broadcast media or to higher management in companies and organisations, or to external regulatory bodies, they all invariably need some documentary proof of what you are telling them, e.g. a document or memo or advance copy of a report, or photographic images or an email. etc.

Hopefully the following technical (and common sense) hints and tips will make you think about whether you are properly protecting yourself or your anonymous sources, given the complexity and power of modern communications and the means to snoop on them.

This is an ongoing Work in Progress, and some of the sections are placeholders, with further details to follow, if people are interested, or wish to contribute.

Please feel free to comment on the individual blog postings with error corrections or other suggestions.

Table of Contents

By
wtwu
on June 11, 2011 9:00 PM | Permalink | Comments (0)

Table of Contents

34. Do not try to handle two whistleblowers at once on the same phone or email account
35. Conclusion
36. Further Reading

Whistleblower Anonymity limits

The protection of journalistic or blogging or disgruntled employee sources, is something which should be fundamental to professional journalists or to serious political bloggers, or even senior management within a Government or private sector organisation.

The need to protect the anonymity of such whistleblowing sources is vital, but it is not necessarily something which lasts forever.

It is absolutely vital during the early stages of a "Leak" of a story interesting or politically embarrassing or commercially sensitive information, during the initial contact phases between the whistleblower and the person they are complaining to.

It is vital when the circle of people who know about the existence of the leak story is inevitably increased, when second opinions are asked about the authenticity or importance of any leaked emails, memos, reports, photographs or other evidence which the whistleblower provides in support of their story.

The problems about which the whistleblower is complaining might, in theory be resolved, once an organisation starts to get enquiries from journalists or from senior management or external regulatory authorities, indicating that they know or suspect the existence of a serious problem or scandal.

However, it is more likely that incompetent, ignorant, inflexible, or corrupt politicians, bureaucrats or systems, will not magically heal themselves in secret, and will only take action when widespread publicity threatens to embarrass someone in power, or more accurately, when it reaches a crescendo which the internal colleagues, rivals and enemies of those in power might be able to use to their own political or financial advantage.

This usually means that the desperate whistleblower has to be willing go public at some point, with some or all of their allegations, after publication in the press, or after a formal Employment Tribunal complaint etc.

In theory the Public Interest Disclosure Act 1998 is meant to protect disclosures by whistleblowers, through the chain of senior management, and, if necessary to external regulators, or Government Ministers, or even the press and media.

1) In this Part a "qualifying disclosure" means any disclosure of information which, in the reasonable belief of the worker making the disclosure, tends to show one or more of the following--

(a) that a criminal offence has been committed, is being committed or is likely to be committed,

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur,

(d) that the health or safety of any individual has been, is being or is likely to be endangered,

(e) that the environment has been, is being or is likely to be damaged, or

(f) that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

Within international Financial Institutions which comply with the US Sabarnes-Oxley Act, there are meant to be anonymous channels of complaint to senior management, available to all employees, sub-contractors and suppliers, typically a supposedly anonymous internal email account.

In theory, no adverse action is legally permitted against such whistleblowers, e.g. affecting their promotion prospects or being fired from their jobs.

In practice, this whistleblower legal protection does not appear to work very well, if at all.

This deliberately weak and narrow Act has done nothing to protect recent UK Government whistleblowers such as Steve Moxon, whose revelations about the immigration scandals at the incompetent Home Office led, eventually to the resignation of the Immigration Minister Beverly Hughes. Neither did it prevent the the smearing and persecution of Foreign Office whistleblowers like James Cameron, the former British consul in Romania, or Craig Murray the former UK Ambassador in Uzbekistan.

If you are a junior or even senior Civil Servant working for the United Kingdom Government, who contacts the press or broadcast media or even political bloggers with a story, the recently revised Civil Service Code of Conduct could be used to damage your career.

See - Minor changes to the Civil Service Code might affect whistleblowers

Somehow this Code never appears to apply to the Political Special Advisors, media spin doctors or other cliques of political appartachiki which the politicians in charge surround themselves these days.

There, of course, also the Official Secrets Act 1989 which has been used to legally harass, but **not** to actually convict some recent whistleblowers such as Katherine Gun (who leaked the GCHQ memo about the bugging of United Nations diplomats in New Yorkp) and Derek Pasquill (who leaked FCO letters and memos about the UK Government policy regarding secret CIA rendition flights and contacts with Muslim groups.)

See the articles in the left of centre New Statesman magazine, which explain the journalistic fact checking and legal case background of the Katherine Gun and Derek Pasquill cases.

- Katherine Gun: The woman who nearly stopped the war by Martin Bright
- I had no choice but to leakby Derek Pasquill

Similarly the whistleblower Lana Vandenberghe and ITN tv news journalist Neil Garrett involved in the leaks of the Independent Police Complaints Commission Inquiry into killing of Jean Charles de Menezes by the Metropolitan Police at Stockwell Tube station, following the bureaucratic official panic, after the failed terrorist bomb attacks of July 21st 2005, were hunted down, and arrested. but not eventually charged with any crime.

The scandal of the bugging of Sadiq Khan MP and his constituent Babar Ahmad, in Woodhill Prison, and the likely bugging of other legally privileged conversations, was only brought to light after retired Detective Sergeant Mark Kearney, the Thames Valley Police officer who conducted the Intrusive and Directed electronic surveillance, and Milton Keynes local newspaper journalist Sally Murrer had already been put under surveillance themselves, and then charged with misconduct in public office, over

alleged leaks of minor local crime stories to the local newspaper. The obvious conclusion is that these proceedings were actually simply to apply pressure to cover up the secret bugging scandal.

See the Daily Telegraph : Hundreds of lawyers 'bugged on prison visits'

Remember, that these days, being arrested by the Police is a severe ordeal and punishment in itself, which involve photography, fingerprinting, palm printing, DNA sampling etc. , by force if necessary. All this data is retained in computer databases, effectively forever, even if you are never charged, or never found guilty of anything, unless you really fight to have it removed.

The details of this prison bugging scandal were first revealed not to the press, but, quite rightly, to a Member of Parliament, who then passed on his fears that the Wilson Doctrine was being breached to David Davis, the Conservative Shadow Home Secretary, who then contacted the Prime Minister (in charge of bugging of MPs)

Then, once the media eventually printed the story, this whistleblower's anonymity was gone, certainly so far as his former colleagues in the Police were concerned, and Mark Kearney chose to give some public interviews.

However, during the crucial time when some external scrutiny was bringing the matter to the attention of the very senior management (ineffectively, as it turns out in this case) , the anonymity of the whistleblower was preserved.

The cases where a whistleblower's identity remains secret for many years after the fuss about the scandal seem to be rare, e.g. the identity of the Washington Post reporter's Bernstein and Woodward source "Deep Throat" whose revelations about the Watergate cover up scandal which eventually led to the down fall of US President Richard Nixon.

Currently, the identity of whistleblower source attributed, perhaps deliberately misleadingly, to the Crown Prosecution Service, who leaked details of the progress of the Police investigation into the "Cash for Honours" scandal involving former Labour Prime Minister Tony Blair and his fund raiser Lord Levy, remains private, so **whistleblower anonymity is possible, even under intense political scrutiny**.

Mole Hunts

Interestingly, the Security Service MI5 claim to be party politically neutral, and that they do not get involved in Whitehall Leak Inquiries and "mole hunts" (a phrase popularised by the espionage fiction novellist John le Carré), unless national security is threatened.

7. MI5 investigates Whitehall "leaks"

We do not carry out inquiries into leaks of information from Government, except where national security may be affected. As part of our protective security role, we do give advice to Government on security policy and practice and our Centre for the Protection of National Infrastructure (new window) carries out audits of security arrangements within other Departments on request. But we have no "policing" role.

A Whitehall Department may well have enough personnel and technical resources to conduct their own mole hunt to try to track down an anonymous whistleblower who is, for example, providing a newspaper with more than one "scoop" based on internal Whitehall documents.

In recent years the Sunday Times has had access to several high profile leaked Whitehall documents via the contacts of David Leppard, (See the **Trustworthy Contacts for Whistleblowers ?** section) who is soon moving on to become

In 2004, the Home Office employed the private sector financial investigators Kroll Associates in their Leak Inquiry following th e publication of Cabinet Committee memos showing the then Foreign Secretary Jack Straw's doubts about the the Home Secretary David Blunkett's notorious ID Cards and National Identity Register plans.

When details of the Honours List were leaked from the Cabinet Office, agin in 2004, another firm of private investigators, set up by retired MI5 people, called Risk Analysis (UK) Ltd was called in:

Investigation & Litigation Support

[...]

In addition to undertaking the more usual types of investigation, Risk Analysis also **provides investigators who are experienced in tracing the origins of confidential information leaks from corporate entities and public bodies**. They act swiftly, sensibly and analytically, and can conduct enquiries openly or discreetly as required.

Surveillance threats to bloggers, investigative journalists and political activists

Some of the current threats to the freedoms and liberties of bloggers, investigative journalists and political activists, who really do need to take some of the precautions suggested in this Hints and Tips guide, to protect themselves and their contacts, from state and corporate and criminal snooping:

- See the articles in the left of centre New Statesman magazine, which explain the journalistic fact checking process and legal case background, of the Katherine Gun and Derek Pasquill cases which both involved (eventually) dropped prosecutions under the UK Official Secrets Act 1989:
  - Katherine Gun: The woman who nearly stopped the war by Martin Bright
  - I had no choice but to leak by Derek Pasquill
- Counter-Terrorism Bill Clause 83 - chilling effect on reporting or speculation about military or intelligence service or police personnel ?

  This amendment, contained in the Counter-terrorism Act 2009 section 76, has created the new Terrorism Act 2000 section 58A Eliciting, publishing or communicating information about members of armed forces etc, and is now fully in force.

- Remote Searching of Computer Hard Disks - remember that RIPA etc. do not protect business premises from arbitrary intrusive surveillance, property interference etc.
- Even correspondence between Members of Parliament and whistleblowers or Parliamentary Constituents is under threat, as the **arrest** of Conservative MP Damian Green, and the **searches without a warrant** of his offices, and, in a separate incident, the office of Conservative MP Daniel Kawczynski show.

  See:

  - Exactly what correspondence or communications between MPs and their Constituents is protected by Parliamentary Privilege ?

    - Wilson Doctrine and Parliamentary emails and the arrest of Damian Green MP
    - Conservative MP Daniel Kawczynski - parliamentary office searched and constituency correspondence handed over to the Police, without a warrant - updated
- Serious Crime Act 2007 used to harass Indymedia server colocation administrator - updated
- The Guardian reports that **innocent** peaceful political demonstrators and activists, and even the mainstream media journalists, tv camera crews and photographers are being snooped on, and having their details stored in and shared in Police criminal and other intelligence databases.

    Revealed: police databank on thousands of protesters

    Films and details of campaigners and journalists may breach Human Rights Act

    * Paul Lewis and Marc Vallée
    * guardian.co.uk, Friday 6 March 2009 19.30 GMT

    Shocking footage shot by police, accompanied by their own critical commentary, shows how their officers monitored campaigners and the media - and demanded personal information - at last August's climate camp demonstration in Kent

    Police are targeting thousands of political campaigners in surveillance operations and storing their details on a database for at least seven years, an investigation by the Guardian can reveal.

    [...]

    The Guardian has found:

    •Activists "seen on a regular basis" as well as those deemed on the "periphery" of demonstrations are included on the police databases, regardless of whether they have been convicted or arrested.

    •Names, political associations and photographs of protesters from across the political spectrum - from campaigners against the third runway at Heathrow to anti-war activists - are catalogued.

    •Police forces are exchanging information about protesters stored on their intelligence systems, enabling officers from different forces to search which political events an individual has attended.

    [...]

- The Guardian reveals details of the mechanics of the failed Hotmail plot by the anti-Gordon Brown faction of Labour MPs

    Why plot to oust Gordon Brown failed

    The rebels switched from email to texts on a disposable mobile but bid to oust PM was doomed

    * Allegra Stratton, political correspondent
    * guardian.co.uk, Wednesday 10 June 2009 21.48 BST

> [...]
>
> One rebel said: "We got one email from brownn@parliament.uk [the email address of the chief whip]. It might be that they were hoping we'd publish a list and not notice his name was in it and then he could show all the names were ridiculous."
>
> [...]
>
> Instead, the rebels adopted a tactic favoured by organised criminals and bought an untraceable pay as you go mobile, encouraging sympathetic colleagues to get in touch that way. It became a text message plot.
>
> [...]
>
> One cabinet minister due to meet a rebel for dinner had their meeting cancelled - there simply wasn't a restaurant in London discreet enough.

It certainly looks as if the failed "Hotmail plot" anti-Gordon Brown faction of Labour MPs suspected that they might be under political surveillance.

tor2web.org/

Technical ineptitude - the "bomb Al-Jazeera memo" leak

Here is an example of how **not** to leak sensitive Government documents to the public:

The Tony Blair / George Bush "bomb Al-Jazeera" memo leak case involving former parliamentary researcher Leo O'Connor, and former civil servant communications officer at the Cabinet Office David Keogh, who were convicted in 2007 , under the Official Secrets Act, after passing the leaked memo, back in 2004, to the then Labour MP for Northampton South, Tony Clarke, who lost his seat at the next General Election in 2005.

Also implicated is former Labour junior Defence Minister Peter Kilfoyle, MP for Liverpool Walton, who, despite claiming that he had not seen the actual memo, tried to pass its contents on to the Democrat Presidential candidate Senator John Kerry's campaign team in the run up to the 2004 US Presidential Election. The did not make use of this, either because they thought it might actually help President Bush in his reelection campaign, or, because they had no way of properly authenticating the memo.

Apart from their political naivety, the mechanics of the actual whistleblower leaking, and the subsequent Police investigations described by the press, shows **a surprising lack of "tradecraft"** by the civil servant and the political researcher, and **ignorance** of the possibilities of the **internet**, of **forensic document examination** techniques, of **mobile phone communications traffic data** etc

It also demonstrates **very lax security** at the Cabinet Office fax machine room - how was it physically possible to smuggle a document marked "Secret" out of the building ?

Daily Mail
Facing jail, the civil servant who leaked Bush-Blair secrets,
By BETH HALE and LAURA ROBERTS
Last updated at 23:22pm on 9th May 2007

[...]

But the jury heard that Keogh leaked the **four-page document** because he believed it exposed Mr Bush as a "madman".

[..[

The events leading to the trial began when Keogh, 50, was working alone in the Government's high-security Cabinet Office Communications Centre and a document rolled out of the fax machine marked "secret" and "personal".

It detailed talks on the war in Iraq between Mr Blair and Mr Bush and some of their most senior advisers in Washington in April 2004.

Among the limited detail that was made public was the line: "This letter is extremely sensitive. It must not be copied further. It must only be seen by those with a real need to know."

Keogh was so shocked by the contents of the document that he wanted it to be raised in the House of Commons and passed on to U.S. presidential candidate John Kerry.

He gave the document to O'Connor, 44 - a researcher for anti-war MP Anthony Clarke - who placed the memo in the MP's paperwork.

Why was it physically possible for Keogh to walk out of the building with a document marked Secret ?

But their plans were foiled when Mr Clarke handed the document over to Downing Street.

Keogh, a civil servant since 1979, had met O'Connor at a dining club in Northampton, of which Mr Clarke was also a member.

He first showed O'Connor a copy of the document over a drink at the town's Labour Club. Later the two men copied the fax.

The original was put back in the in-tray at Whitehall and O'Connor kept the copy.

Keogh said he thought O'Connor would have the contacts to get maximum publicity and that far from damaging British troops, the document would simply embarrass Bush.

By contrast O'Connor had claimed to have been terrified, and wanted to get it back to its original home.

His method was to conceal the documents in Mr Clarke's papers and later to tell police he hadn't "got a scooby" how it had got there.

[...]

O'Connor's claim sounds ridiculous - why would returning the document to Downing Street via an MP or even the Parliamentary internal mail system not immediately tip off the Cabinet Office that a Secret document had gone issing ?

If Keogh could smuggle the document out, then surely he could smuggle it back in to the secure area, if necessary ?

The Times has some more details of the forensic methods used to establish proof of the involvement of Keogh and O'Connor in the whistleblower leak, although, probably by that stage, their identities were actually known by the Police.

The Times
April 19, 2007 Blair aide 'leaked classified Iraq memo'

Michael Evans, Defence Editor

[...]

Mr Perry described how the police tracked down the source of the leak. The meeting between Mr Blair and Mr Bush took place in Washington on April 16, 2004, when Iraq was under the control of the US-led Coalition Provisional Authority. The record of the meeting, drawn up by Matthew Rycroft, Mr Blair's private secretary for foreign affairs, was sent by letter to Geoffrey Adams, private secretary to Jack Straw, then the Foreign Secretary.

The letter was faxed through to the Pindar communications centre, a Cabinet Office facility, where Mr Keogh was on duty when it arrived.

House of Commons Hansard 29th April 2004, Column 392

"Mr. Hanley : The PINDAR facility is located beneath the Ministry of Defence main building in Whitehall. Details of its size and layout are of an operational nature and it is not our practice to reveal such information."

The letter was to be given limited circulation because of its sensitivity. Those on the need-to-know list included Sir David Manning, Ambassador to Washington; Sir Nigel Sheinwald, the Prime Minister's foreign policy adviser at No 10; John Scarlett, chairman of the Joint Intelligence Committee (now head of MI6); Jonathan Powell, Mr Blair's chief of staff; and David Hill, Downing Street's director of communications. It was also sent to the British representative to the UN and to David Richmond, Ambassador to Iraq.

Mr Perry said that the police were alerted to a possible leak when a copy of the secret document turned up in a pile of papers belonging to Anthony Clarke, then the Labour MP for Northampton South.

Mr O'Connor, who worked for the MP, had "slipped" the document into the other papers. Mr Perry said that the document was passed to Mr Clarke in the hope that it would be given wider circulation. The Labour backbencher had voted in 2003 against invading Iraq. The document was passed to the Special Branch.

All copies of the document were traced and retrieved, and **scientific examination proved** that the copy that ended up in Mr Clarke's constituency office in Northampton was a copy of the fax that originated at the Pindar communications centre. Further tests revealed **Mr O'Connor's fingerprints** and **a trace of his handwriting, which had come through as "dents" on the document after it had been placed in an envelope** with Mr Clarke's name written on it.

Contact between Mr Keogh, who was said to be "bored to tears with Iraq", **and Mr O'Connor**, who claimed to police that he was "95 per cent behind the military action against Saddam Hussein", **was uncovered when the police examined mobile phone calls and text messages between the two.**

Trustworthy Contacts for Whistleblowers ?

Unless you are making use of something like the defunct (so far as new submissions are concerned) WikiLeaks.org (see the Leak Directory wiki for possible alternatives) , or are using a scattergun approach by, sending anonymous letters or emails to a wide range of journalists, on a speculative basis, in the hope that they will somehow drop all their other work and concentrate on your leak, it may well be worth making informal, discreet contact with some people to whom you make choose to leak something in the future.

The scattergun speculative approach also runs an increased risk of "tipping off" your employers or the authorities about a leak, even before you have had any benefit of any publicity for the story. They may then instigate a Mole Hut or Leak Inquiry to try to track you down as a political damage limitation exercise, even if it is only a case of "going through the motions", to Pretend To be Seen To Be Doing Something, in order to protect "officially sanctioned leaks" and confidential briefings to the very same media organisations, when it suits the apparatchiki spin doctors and politicians.

Obviously if journalist, bloggers or independent regulators are under surveillance, which, does seem to be the case sometimes, then you need to take as much care with these initial, non-incriminating contacts, as when you do have something juicy to hand over to them later.

Here are some media and blogger contacts for, primarily UK Government Whistleblowers, who have some track record of discretion and actual wider publicity generation.

In no particular order of trustworthiness:

- Guido Fawkes - Paul Staines - political gossip blog (unfortunately with many stupid and nasty anonymous comment contributors) which is widely read by "Westminster Village" journalists and politicians,
- The Register - required reading for Information technology and privacy / surveillance state related news stories -
  John Lettice, John Leyden, Chris Williams
- British Broadcasting Corporation - various radio and tv and web journalists, but they cannot pay for any stories.
- The Sunday Times - David Leppard
- The Guardian - David Hencke
- The Daily Mail / Mail on Sunday - Jason Lewis
- Evening Standard - Andrew Gilligan
- ~~WikiLeakS.org~~ [no longer accepting submissions]
- The Guardian , The Observer and Vanity Fair - Henry Porter - one of the organisers of the Convention on Modern Liberty.
- David Davis MP - Conservative former Shadow Home Secretary - various Home Office immigration scandal whistleblower leaks
- Dr. Vincent Cable MP - Liberal Democrat Treasury spokesman - various Treasury and Banking whistleblower leaks, Parliamentary Questions about the "Wilson Doctrine" regarding the confidentiality of MP's constituency correspondence etc. [N.B. he is now a Government Minister, a position which seems to have silenced him on these issues]

There is also a role for Trusted Intermediaries and Middlemen, to act as cut outs, between the media and a whistleblower, especially if monetary payments are being sought.

Contact Spy Blog if you want us to suggest and pass on your details to some journalists, or bloggers, or other ombudsmen, regulators or politicians who we have had dealings with before.

email: blog@spy.org.uk

Spy Blog - PGP Encryption Key

Whistleblower middlemen, intermediaries, cut outs

In very high profile whistleblower leak cases, especially were some sort of monetary payment is sought from the mainstream media, it is common to make use of middlemen or intermediaries who act as a cut out between the media and any leak investigators and the real whistleblower source(s).

The leak of the uncensored details of expense claims by UK Members of Parliament, which was brokered around several newspapers, before being taken up by the Daily Telegraph, illustrates this.

See Spy Blog Naming of the MP Expenses whistleblower leak intermediaries ?

The Times has some more details about the role of this intermediary:

From The Times
June 12, 2009

John Wick, middleman who passed on MPs' expenses, on why he fled the UK

Security expert John Wick says he wants all erring MPs exposed, regardless of their party

Dominic Kennedy and Steve Boggan

The security expert who brokered the leak of MPs' expenses secrets has said that he fled Britain fearing arrest for theft and stayed abroad until Scotland Yard announced that there would be no investigation.

John Wick, 60, an ex-SAS major, insisted that he was just a middleman and was deliberately unaware of the identity of the mole who removed more than a million computerised Commons documents.

[...]

Mr Wick says he accepted assurances that none of the material he provided to *The Daily Telegraph* had been stolen by the mole. But he admitted that he fled to Spain as the story was published, having consulted his lawyer about the risks of a police investigation into the leak. "There are several possible potential crimes all with different likelihood of the Crown Prosecution Service doing anything about it and all with different punishments and different defences," Mr Wick said.

He and his communications consultant, Henry Gewanter, who sat through the interview, mentioned theft, fraud, aiding and abetting, the Terrorism Act and breaching state secrets. Mr Wick said: "**The deal was with the people [behind the leak] that if there was a problem I would have to go to court and I would have to defend myself and not disclose them so if I went down, I went down.**

[...]

"As soon as the thing went out I left the country because I could run it, look after the sources and run everything I had to do with The Telegraph from outside the UK while it just settled down.

"I only came back when the Commissioner let it be known that he was not interested in me."

Mr Wick said he adopted a blind approach to the mole so that, even if he ended up in a police cell or courtroom, he could honestly deny knowing who had accessed the secrets.

[...]

The go-between was acting on behalf of the original anonymous source. Mr Wick said: "I was told it was not stolen. I was told it was a copy that had been made without anybody really realising it because of lax controls in Parliament."

[...]

This sort of espionage tradecraft cut out is probably also still necessary even if little or no money is to change hands , in order for the whistleblower leak to be made public as widely as possible, without destroying the whistleblower source's anonymity.

As in this case,it may require more than one middleman or intermediary, one to handle the confidential "dead drop" arrangements with the whistleblower source, and another to actually contact and negotiate with the mainstream media publications etc.

Suggestions of how to contact such Trusted Intermediaries, in confidence, are welcome. - see Trustworthy Contacts for Whistleblowers ?

What to do if you are arrested as a whistleblower

Get proper legal advice immediately

Here in the United Kingdom, there are now some very repressive laws which could be used to legally harass, intimidate or actually arrest , prosecute, convict and imprison whistleblowers. e.g. Official Secrets Act 1989, Terrorism Act 200, Terrorism Act 2006, Counter Terrorism Act 208, Serious Crime Act 2007 etc.

There are some "public interest" defences but these generally only apply once your case has actually got so far as a Court or at least a pre-trial legal hearing before a Judge.

By this time you may well have been arrested, fingerprinted, DNA sampled, photographed, and had all of your home and business premises searched, and mobile phone and computers and paper documents seized etc.

The very first thing you should do is get some proper legal advice from some solicitors who are well versed in Police arrest and search procedure, human rights and data protection laws, legal aid and potentially long running legal appeals.

Say nothing to the Police or other "investigators" until you have contacted a proper legal advisor.

This also applies if you have not yet got to the stage of actual Police involvement, just an "internal" leak inquiry conducted by your employer.

Most people do not have the phone number of a firm of solicitors to hand, but whistleblowers, investigative journalists, and writers, bloggers and political activists should take the precaution of researching a few contacts, and keeping them in their mobile phones and address books etc.

N.B. as David Mery points out in the comments, you are unlikely to be allowed to use any mobile phones or electronic PDAs etc. if you are arrested, so you should **also** keep the contact details for firms of Solicitors **printed out on a bit of paper** in your wallet etc.

A couple of London examples of such reputable, expert firms of solicitors, who offer a round the clock telephone contact hotline (remember that you are likely to be arrested via a "dawn raid") :

- **Bindmans - telephone: 020 7833 4433**

  Bindmans LLP
  275 Gray's Inn Road
  London
  WC1X 8QB

  DX: 37904 King's Cross

  Tel: +44 (0)20 7833 4433
  Fax: +44 (0)20 7837 9792
  Email: info@bindmans.com
  Web: www.bindmans.com

- **Kaim Todner - telephone: 020 7353 6660**

  Kaim Todner LLP

  http://www.kaimtodner.com/about_us/how_to_contact_us.asp

  For general email enquiries: solicitors@kaimtodner.com

  5 St. Bride Street
  LONDON
  EC4A 4AS

  Tel: 020 7353 6660
  Fax: 020 7353 6661

  DX: 265 LONDON CHANCERY LANE

We welcome any recommendations of similar firms in other parts of the United Kingdom.

Get witnesses to record your arrest or any searches

Get a friend or family member to take notes, photograph, record or video (perhaps on a mobile phone) , as much of your arrest and / or search of your home or business premises as possible.

Post arrest media publicity

If there is a genuine Public Interest in your whistle blower leaks and revelations, then the mainstream media and online media publicity may well be the deciding factor in whether you are prosecuted or not.

The "shoot the messenger" tendency of bureaucrats, politicians and other people in power is as old as history, but they are less likely to do so under the glare of publicity.

See

- Trustworthy Contacts for Whistleblowers ?

Secure computer configuration checklists and scripts etc.

Before you can make sensible use of your computer system, to help you with your honourable whistleblowing or investigative journalism or political blogging or activism, you need you create a **Secure Computing Base**.

Do not neglect the physical security of your office or home e.g. locks, alarms etc.

You can then "harden" your computer, to provide a secure foundation on top of which you can add standard firewalls, anti-virus and anti-spyware software, security enhanced versions of web browsers, and more advanced encryption and anonymity tools.etc.

For most computers, i.e. those running versions of Microsoft Windows operating systems, this means changing quite a lot of the default installation options.

A well configured Windows system is at least as "secure" as the less popular Apple and Linux systems, no matter what the marketing hype and the fanbois claim .

The US Government tries (not always successfully, due to human incompetence or corruption) to secure its millions of personal computers and networks. They do publish checklists, guides, configuration templates and scripts etc. to help to do this. for Windows, and for other systems such as Cisco routers as well. There are also checklists for popular applications software such as the Microsoft Office suite etc.

National Institute of Standards and Technology (NIST):

- Federal Desktop Core Configuration
- National Checklist Program

See also the computer security guides produced for Non Governmental Organisations and political activists / dissidents:

- "Security in-a-Box - is a collaborative effort of the Tactical Technology Collective and Front Line. It was created to meet the digital security and privacy needs of advocates and human rights defenders. Security in-a-box includes a How-to Booklet, which addresses a number of important digital security issues. It also provides a collection of Hands-on Guides, each of which includes a particular freeware or open source software tool, as well as instructions on how you can use that tool to secure your computer, protect your information or maintain the privacy of your Internet communication."
- Digital Security & Privacy for Human Rights Defenders manual, by Irish NGO Frontline Defenders.
- Handbook for Bloggers and Cyber-Dissidents - March 2008 version - (2.2 Mb - 80 pages .pdf) by Reporters Without Borders
- A Practical Security Handbook for Activists and Campaigns (v 2.6) (.doc - 62 pages), by experienced UK direct action political activists
- Anonymous Blogging with Wordpress & Tor - useful step by step guide with software configuration screenshots by Ethan Zuckerman at Global Voices Advocacy. (updated March 10th 2009 with the latest Tor / Vidalia bundle details)

Email and Encryption

Email

1. Do not use your work email address e.g. @homeoffice.gsi.gov.uk to pass on whistleblower material to politicians, journalists or bloggers.

   The Home Office (or other Government Department) , as your employer, is perfectly within its rights to analyse the log files of its own email systems. They do not need to wait for a "serious criminal investigation" which would require a Regulation of Investigatory Powers Act 2000 warrant signed by, wait for it, the Home Secretary, or as recently delegated under the Terrorism Act 2006, any nameless official that the Home Secretary delegates the renewal of long running intelligence agency or electronic interception warrants, which almost certainly include the "protection" of the Home Office IT systems themselves.

2. If you are ~~relatively~~ very IT literate, you may be able to master how to send an email through a Mixmaster Anonymous Remailer chain, but, we suspect that the number of people who are confident enough to do this currently working at the Home Office and who might become whistleblowers is very small.
3. Similarly, a whistleblower could use Pretty Good Privacy public key encryption, but again, this requires some effort to install the PGP software, on your own PC (not on your Home Office workstation !)
4. PGP encryption could **protect the content** of of your correspondence with whoever you are whistleblowing to, **but not the fact that your are in communication** with say, David Davis, or the Sun newspaper or even a political blog.
5. GPG - Gnu Privacy Guard is an open source version of PGP, compatible with most PGP keys (and vice versa), except for some of the old keys which used RSA public key and IDEA symmetric key algorithms, which the open source purists did not want to use, due to their patent status, despite "free for non-commercial use" licences.
6. Unfortunately it is only Spy Blog and a few other technical security and privacy related blogs which publish a PGP Public Encryption Key, something which we encourage other bloggers, journalists and members of Parliament to do as well. - Spy Blog PGP public encryption key

Hushmail

A good compromise for the non-technical civil servant who wants to be a whistleblower could be a Hushmail account.

This has the advantage of being based in Canada, Ireland and the tax haven of Anguilla, and is a web based email system which uses the SSL/TLS encryption used to protect credit card and internet banking transactions from snoopers.

You may have to install the Sun version of the Java Runtime Environment if you have a recent version of Windows XP which no longer comes with Java installed by default.

- Hushmail, as of mid-October 2006 now have a "No Java" or "Turn Java Off" option in their web page client. The encryption gets done at the server. The web browser to web server SSL/TLS https sessions remain, but are therefore at risk of a man-in-the-middle attack, whilst being immune from casual monitoring.

You can sign up for a free, anonymous Hushmail account, (with 2Mb of storage space) which needs to be accessed at least every 3 weeks to keep it active . You can pay about US $35 a year for a full account,which gives you a Gigabyte of email and document storage, and the very useful ability to create email aliases e.g. ht4w@nym.hush.com, (but obviously this will leave a credit card trail with your name and address, unless you use the hard to trust e-gold payment system).

Hushmail to Hushmail traffic is strongly encrypted, but using Hushmail to say, email your Member of Parliament will be plaintext like other emails.

Hushmail do have a "pre-shared secret" challenge/response email system called Hushmail Express which can be useful for non-hushmail replies, but it is quite a bit less secure, although still a lot more secure than unencrypted email.

Whether or not it is safe for a whistleblower to use a Hushmail account from within their workplace, depends on the situation. Ideally this should be done from home or even a public cyber café etc. (unless the whistleblower feels that they are under directed surveillance i.e. being followed or observed).

Hushmail obviously complies with Canadian law

Hushmail have handed over emails probably stored in the online mailbox, and IP address logs as a result of a Canadian Court Order, at the request of the US authorities who were investigating a relatively minor anabolic steroid drug dealer.

Deleting your stored emails after you have read them, and always using the Java applet, still makes Hushmail more secure against electronic interception, than the more common web based email services.

See *Wired* magazine's investigation: Encrypted E-Mail Company Hushmail Spills to Feds

See also the April 2010 *Wired* article about the case of a senior US National Security Agency accused of leaking information to a *Baltimore Sun* newspaper reporter NSA Official Faces Prison for Leaking to Newspaper

[...]

Thomas Andrews Drake, 52, was a high-ranking NSA employee with access to signals intelligence documents when he repeatedly leaked classified information to the unnamed reporter, who ran stories based on the leaks between February 2006 and November 2007, the indictment alleges.

Fox News is reporting that the journalist was Siobhan Gorman, who worked at the time for the *Baltimore Sun* and is now a reporter with *The Wall Street Journal*, which is published by Fox parent corporation News Corp.

According to the indictment, Drake exchanged hundreds of e-mails with the reporter, and the two met in the Washington, D.C., area half a dozen times. Drake also researched stories for the journalist, sending e-mail to other NSA employees asking questions, and accessing classified documents to obtain information.

Drake even "reviewed, commented on, and edited drafts, near final and final drafts" of the reporter's articles, according to the government.

[...]

Drake opened a Hushmail e-mail account to contact Gorman, and volunteered to provide information about the NSA. Drake instructed the reporter to open her own Hushmail account so they could communicate covertly.

Hushmail is a Canada-based encrypted e-mail service that allows account holders to communicate securely with a client-side Java encryption applet. But Threat Level previously reported that the company has subverted its own encryption to help U.S. and Canadian authorities gain access to customer e-mail, in response to court orders. It's unclear if the FBI used that capability in investigating Drake.

Gorman agreed that information gathered from Drake would be attributed in articles to a "senior intelligence official" and that Drake would never be her only source for information.

[...]

The fact that a senior NSA official chose to trust Hushmail for his whistleblowing activities, is some sort of endorsement.

The proviso that he should not be the only source for any newspaper articles, is a wise one for whistleblowers dealing with the mainstream media.

However, perhaps "hundreds of emails" exchanged for more than a year, was rather too much use of that particular channel of communications ?

Presumably the FBI were snooping on all of the *Baltimore Sun* journalists, in order to try to track down the source of the NSA internal leaks ?

Hushmail and PGP

If you encrypt or sign and encrypt a message using your own PGP or GPG software, and then also use Hushmail to encrypt and or digitally sign your PGP message block inline in the body of the email, rather than as an attachment, this seems to cause problems for some versions of GPG software, due to an extra "-" and and extra " " space at the start of the encrypted block. Windows PGP software handles this ok, but various Linux open source and Apple versions of GPG do not. Either dispense with using

Hushmail's digital signing, if you are already encrypting and signing with your local PGP key, or put any such messages or files into attachments rather than the inline body of the email message.

Please note: Hushmail only recognizes digital signatures on text messages that are signed using the Cleartext Signature Framework as described in RFC2440 section 7. Thus when sending to a Hushmail account you must sign the message first, generating a cleartext signed message, and then encrypt the result. If you encrypt and sign a message in a single step (the default for many PGP applications), the signature will not be recognized.

Gmail sessions are now encrypted by default

In response to the Chinese government hacking attacks on human rights activists Google gmaill accounts, the search engine giant has now (January 2010) switched on **https://** SSL / TLS encryption **by default**.

See The Register article Google flips default switch for always-on Gmail crypto

Google mail also understands STARTTLS encryption between mail servers, so, for example a Gmail to Hushmail message will be encrypted all the way through, making interception by anyone other than the US or Canadian authorities unlikely.

Note that you Gmail Inbox and Sent folder, will still be **unencrypted**, and will be keyword searched by Google search engine software for Advertising Keyword (or Government watchlist) purposes.

Encryption does not mean Anonymity

Sending an email message which has been encrypted with PGP, or through a fully encrypted email service like Hushmail, or (now) mostly) encrypted one like Gmail, should preserve the Privacy of **what** is being sent, but it does **not** necessarily protect the **anonymity** of the whistleblower i.e. the **when** and **to whom** it was sent.

Neither Gmail to Hushmail, nor any other email system is immune from **Communications Traffic Data** retention, snooping and analysis i.e. which email account communicated with which other account, at what date and time, and how big a message was sent (which may be indicative of attached whistleblower documents etc.)

Obviously if you pay for an email service, especially through a Credit Card, then there will be a financial audit trail leading back to you.

Luckily, many "free" email accounts are available (with obviously limited functionality compared with the paid ones).

It is possible to set up a free Hushmail or Gmail or Hotmail or Yahoo mail etc. account, even through anonymising proxy services or Tor.

Such accounts based outside of the United Kingdom , and so make it more of an effort for the UK authorities to snoop on such email systems legally, especially during a whistleblower leak investigation, which does not qualify as being serious enough to invoke the national security ofr serious organised crime proportionality test under the Regulation of Investigatory Powers Act 2000 section 81 General interpretation

(3) Those tests are--

(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;

(b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

STARTTLS

Wikipedia article on STARTTLS

STARTTLS is an extension to plain text communication protocols. It offers a way to upgrade a plain text connection to an encrypted (TLS or SSL) connection instead of using a separate port for encrypted communication.

STARTTLS for IMAP and POP3 is defined in RFC 2595, for SMTP in RFC 2487, and in RFC 4642 for NNTP.

A typical email header between two email servers which are using STARTLS encryption would include lines such as:

(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(No client certificate requested)

EnigmaMail and OpenPGP

There is an easy to install **plugin for the Mozilla Thunderbird email client** called EnigmaMail. which is ,as it describes itself quite a "simple interface for OpenPGP email security"

This needs a copy of the Open Source version of the PGP software, available as a free free download from the Gnu Privacy Guard website.. Obviously there is source code for you to compile your own binary executable programs, and cryptographic checksums to show if the software has been tampered with etc.

However, for most of the people who are reading this article, there is GnuPG 1.4.10b compiled for Microsoft Windows. which is also easy to install.

The EnigmaMail setup wizard allows you to quickly generate a reasonable settings for generating your email encryption and signing key, and the software works well to import the PGP public keys of your correspondents, or to look them up on public PGP keyservers.

If you have difficulty in accessing the official websites for this software, then copies of the EnigmaMail plugin for Thunderbird 3.0 and the GnuPG software for Windows are available for download here.

General tips about encrypted email

1. Remember that the Subject line of your email or the original Filename of any Attachment **may not be encrypted**, and may betray clues to a whistleblower leak investigation. Use something neutral for both of these, e.g. Attachment .doc , Attachment2.doc etc.
2. Do **not** leave the Subject line Blank. Do **not** use anything that looks like spam e.g. "Viagra" or "Designer Watches" or "Poker" or "Important - Please read immediately" etc. as it might well be filtered out before it gets to your intended recipient.
3. For extra security, do **not** store or write down your Email password or Encryption / Decryption passphrase, but **memorise** it.
4. Choose a Strong Password or passphrase.
5. As with many other web based services, if your Web Email service offers a "**Forgotten Password**" or Password Recovery or Reset option, then make sure that Answers to the Challenge / Response Questions are at least as strong as your actual password e.g. if the Question is "What is your mother's maiden name ?", you usually do **not** actually have to reply **truthfully**, or with a very short , easily guessed or easily password cracked answer. US Vice-Presidential candidate Sarah Palin's Yahoo email accounts were illegally accessed in this way in 2008.

Stored Email inbox and outbox

The laws in the UK and the USA and other countries, which protect unwarranted interception of email communications, are very specific,and really only apply to the actual email message in transit.

If your email is stored as a draft, awaiting to be sent, or copies are left **undeleted** in your inbox or outbox, either on your personal computer or on, for example a web based email service on like Hotmail, then the Police and Intelligence agencies **do not** usually need to get an **Interception warrant**, especially if they physically "seize" copies of the personal computer or email server hard disk storage systems for analysis.

Paradoxically, as was shown in the recent proper legal Operation Algebra investigation into child rape criminals in Scotland, shows that the UK authorities **do not** actually need to apply for any Court Order or get a warrant signed by the Home Secretary in order to get access to **Foreign based** email systems, e.g. Microsoft's Hotmail, based in California, USA.

See Spy Blog Operation Algebra child rape convictions in Scotland: open WiFi tracking, digital camera image forensics

Rennie's identity was revealed only after DI's Hood's team had invoked the International Mutual Assistance Treaty, which enabled Scottish investigators to request assistance from their American counterparts. An intervention by the FBI enabled the Edinburgh detectives to place a "preservation order " effectively freezing all the contacts, chatlogs and emails recorded on kplover's email account at the Microsoft offices in San Jose

i.e. although a Court Order in California was involved, this was entirely handled by the US authorities after the **self-authorised Mutual Legal Assistance Treaty request** by the Lothian & Borders Police, in secret, with no independent judicial oversight in the UK.

Obviously this is not much of a issue when dealing with serious criminals, but exactly the same mechanisms, and lack of privacy safeguards would come into play if a "whistleblower leak" inquiry was being handled by the UK Police or other Government agencies.

It would be wise for any whistleblower to make sure that they **do not store copies of emails** which they send or receive, to or from, journalists or bloggers or politicians or external ombudsmen or regulators etc. within their normal email or web mail systems.

Any copies which whistleblowers need to keep, should be in separate, strongly encrypted storage.

There is a technique, which might be effective if a particular email system is not under active surveillance at the time, which has been used since the very start of web based email systems, and which has been used (sometimes unsuccessfully) by terrorist suspects.

This involves composing an email message and storing it as a Draft, on the remote webmail server, but **not** actually Sending it. You then alert your recipient through some other means, e.g. a seemingly innocuous email message using a different account, or an SMS text message or some other sort of "Dead Letter Drop" signal (see Covert Channel Signals for Meetings or Dead Letter Drops

The intended recipient then logs into the same email account (you will have had to have shared the username and password credentials beforehand), in order to read and/or copy the information in the Draft. They will then Delete the Draft email when they have finished with it.

Ideally both the whistleblower and the recipient will have taken steps to hide their true IP Addresses as they access the web email site (see Tor - The Onion Router cloud of proxy servers, Open Proxy Servers, Virtual Private Networks etc.)

This technique can be used with many other systems, not just web email e.g. photo sharing or MP3 music sharing, and blogging websites etc.

RIPA and your Cryptographic De-cryption Keys

In the United Kingdom, the Regulation of Investigatory Powers ACt 200 Part III - Investigation of electronic data protected by encryption etc. has **not** been used against terrorists or drug smugglers etc., but it has been used against animal rights extremist activists and against mentally vulnerable people who stand up for their human right of privacy.

Any Police constable, can issue you with a RIPA section 49 notice, demanding either the plaintext of your encrypted files or messages, or the de-cryption key(s) so that they decrypt your intercepted emails, or encrypted computer files, which they have somehow got into their possession (either legally or illegally).

The legislation threatens you with up to 2 years in prison (and /or an unlimited fine) for not complying with such a section 49 notice, or up to 5 years in prison (and/or an unlimited fine), if the magic words "national security" are somehow weaseled into the investigation.

Tey can also impose secrecy over the fact or substance of a section 49 notice - a "tipping off" offence with a penalty of up to 5years and /or an unlimited fine.

This is all very deliberately vague and catch all.

It is a defence to claim that you have **genuinely forgotten the PGP pass phrase**, especially to an old Cryptographic key pair.

Appallingly for justice, the **burden of proof falls on the accused,** who has to prove his or her innocence, rather than be assumed to be innocent , with the prosecution having to prove guilt beyond reasonable doubt.

However, if you can show that you, as a human, rather than a machine, have never known the secret de-cryption key, e.g. for your SSL / TLS encrypted web browsing session, or the transient encrypted OpenPGP links between Tor server nodes or the STARTLS encryption between two email servers which you are not the systems administrator for or any other other ephermeral encryption, then you have a reasonable chance of defending yourself in Court.

Of course, your life will have been ruined by arrest / DNA sampling / Fingerprinting and criminal intelligence database records which are retained for ever, even if you are found not guilty in Court.

Telephones - Pay Phone Boxes or Private Landlines

Telephones - POTS

1. Plain Old Telephone System (POTS) - Pay Phone Boxes or private landlines

   Ever since the days of IRA or INLA bomb attacks and fake bomb hoaxes (designed by the terrorists to cause more panic after each attack, and by malicious or lunatic callers jumping on the media bandwagon) , all the Public Phone Boxes in London can be pin-pointed within seconds (often before the phone call has finished) if they are calling certain phone numbers, including all the main newspaper, tv and radio stations (which is where such "code worded" bomb warnings were usually directed to).

   The same is true for 999/112 Emergency Service calls, which show up immediately they are answered, on a touch screen graphical information system map

   We assume that the Communications Traffic Data for all of these major media outlets is routinely recorded and checked, just in case there is a future terrorist bomb warning or claim or responsibility.

   Many of these organisations will record the calls to their main switchboards and news rooms as well, for just such occasions, and for "news" purposes.

   This also means that any Home Office or other Central Government "leak investigations" will try to use this information to track down any whistleblowers .

   Obviously the same is also true of any home or office land line phone used in the United Kingdom.

2. Do not use your Home Office landline telephone or fax machine for the same reasons as above.

Buying a pre-paid phone card or mobile top up calling credit voucher anonymously

Buying a pre-paid phone card or mobile top up calling credit voucher anonymously

Whistleblowers often need to communicate with potential publishers of their disclosures in private. Cheap pre-paid mobile phones can be valuable for this either for voice calls (ideally using a pre-

arranged code or pre-arranged "beeping" signals) or by using SMS text messages to arrange face to face meetings and / or whistleblower document disclosure drops or deliveries.

Such mobile phones are now cheap enough for a journalist or blogger (or Confidential Human Intelligence Source handler) to give them out to their whistleblower contacts and to pay for the top up calling credit from their end, rather than potentially exposing the identity of their source.

N.B. A whistleblower or other confidential journalistic sources should watch out for the periodic SMS text messages which are supposed to warn a mobile phone user that their mobile handset has been registered with a web based online Location Based Services tracking service - replying to such a message indicates consent for the tracking to continue Any use of such Location Based Services should be agreed up front by both parties. By default all new phones and SIM cards are blocked from using these "Adult" services so you have to contact the network e.g. at a high street mobile phone shop, for them to flag that handset as being usable for tracking (or for expensive SMS or internet pornography or sex chatlines etc.)

However, just because pre-paid mobile phones are often referred to by the Police and by lazy journalists as "anonymous" , that does not mean that they are.

The Communications Data generated by mobile phones is of three types - Location, Friendship tree (or suspect list of co-conspirators) of which number called which other number , when and for how long and your Subscriber Details.

Buying an "anonymous" pre-paid mobile phone only protects your anonymity from the central registration of Subscriber Details i.e. name and address.

1. Expensive, high end smartphones are as powerful as many computers and some models e.g. Apple iPhone attempt to track your usage and identity, especially if you purchase ring tones or music online. Others, like Google Android based phones make a virtue of their Location tracking capabilities. All of these have their uses, but present dangers to a whistleblower trying to contact a journalist or blogger or other intermediary to set up face to face meetings or to arrange whistleblower document deliveries or drops. These phones can cost hundreds of pounds, so they are not usually viable as disposable "burner" phones, unless you are also involved in drug dealing or have a corporate expense account.
2. Buy a basic, cheap **pre-paid** mobile phone from a supermarket etc.. e.g. VX1 Party Phone unlocked Credit Card sized basic mobile phoneSamsung GT-E1080i -a very basic voice and SMS only phone with a long battery life, available for just £9.97 including a free SIM card from one of seven network operators / billing services available from the larger Tesco supermarkets.
3. You can buy a new pre-paid Mobile Phone from, for example, Tesco or Sainsburys etc., for as little as between £10 to £20 pounds
4. Tempting as it is to buy two or more such cheap phones (for the spare battery and power charger alone), do **not** do so from a Supermarket. These often have arbitrary, unpublished or poorly advertised "rationing" policies in place, limiting the number of such "bargain" phones which an individual customer can buy at a time. You do not want the supermarket checkout operator to have to "consult" with the floor supervisor and have to argue about how many phones you are allowed to buy, not if you are trying to remain forgotten and anonymous in case of future whistleblower leak investigations. Obviously if you are getting a trusted third party to buy the pre-paid mobile phone for you, this may be less of a risk to consider.

5. Do **not** buy the phone handset using a Credit Card or a make use of a Supermarket Loyalty Card, both of which will link to your name and address details.
6. Do **not** buy mobile phone top up credit from your own bank Automatic Teller Machine or online bank account

7. Do not top up over the mobile phone e.g. Vodafone 2345, using your own Credit Card / Debit Card.
8. **Use cash** to buy a top up credit voucher from a shop or supermarket, ideally avoiding CCTV cameras.
9. Some mobile phone networks e.g. Orange promote the use of plastic swipe card top up cards, which firstly need to be registered to the SIM card and phone number you are using. Obviously these should normally be avoided, but there may be circumstances where they are useful e.g. if journalist or lawyer or blogger (or Confidential Human Intelligence Source handler) gives a mobile phone to their whistleblower source / confidential contact, they can conveniently top up the phone credit remotely at a supermarket checkout or also via the online website.
10. It is common practice in the Third World for people in cities (where there are mobile phone shops) to purchase mobile phone calling credit vouchers and then to SMS text message the 12 digit one time code number to their relatives who live in country villages etc. Therefore you can and should buy top up calling credit vouchers at several different locations, ideally getting someone else to do so on your behalf.
11. You could get a friend or relative to buy top up calling credit vouchers for you and then communicate the 12 digit code to back to you, using other communications channels. At a push they could phone you up on a different mobile phone and read the numbers off to you, but secure, encrypted email etc. would be better.
12. Do **not** send the 12 digit calling credit top up voucher numbers either via unencrypted, normal, internet email or by SMS text message. Nominally the Interception of the content of such electronic communications would need a warrant signed by the Home Secretary, and it is unlikely that these would be noticed before a whistleblower leak story was published, but they may well be available to a later Leak Inquiry investigation.
13. Do **not** switch on or Activate the new mobile at home or at work, or when your "normal" mobile phone switched on.The first activation of a mobile phone has its physical location specially logged, and it is easy to see what other phones are active in the surrounding Cells at the same time i.e. your own "normal" mobile phone.
14. Destroy the paper copies of any top up calling credit vouchers after you have used them, they are of no use to anyone except a future Leak Inquiry investigator - they give details of time, date location of where they were purchased. The voucher number which can obviously be cross referenced to the SIM card and Phone that they were used to top up. If you are a journalist or police officer etc. claiming the cost of this top up calling credit on expenses, then you only need receipts for the amount of money spent, you should not hand over originals or copies of the actual vouchers themselves.
15. Do **not** Register your pre-paid mobile phone, despite the tempting offers of "free" phone credit.
16. Second hand mobile phone handsets can be bought online, but this obviously leaves a Credit Card or PayPal etc. electronic transaction trail, so do not bother.

17. Second Hand mobile phone handsets are often available at non-mobile phone network shops or at counters within a larger shop, usually offering Mobile Phone Unlocking, repairs, mobile phone accessories like coloured casings etc. and spare batteries and chargers etc. which the mainstream Mobile Phone shops no longer bother with. They often cater to local immigrant communities who have foreign registered mobile phones which they want to use ion UK networks. Phone Unlocking from one network to another is not illegal, but re-programming the IMEI is (up to 5 years in prison even for advertising such a service), because of the legal fiction that stolen mobile phones could only ever be unblocked in the UK, rather than overseas as they have always been.

    The disadvantage with this sort of purchase is that they are often more expensive than a new low end Supermarket phone and they could have been previously used by drug dealers or illegal immigrants etc. who are already being tracked electronically by the authorities. These shops do not usually have extensive CCTV camera video recordings like supermarkets, but they are likely to be regularly questioned by the Police etc. so the shop assistant / proprietor may quickly "cooperate" with any Leak Inquiry investigation, if you are in any way memorable.

Pre-paid cards for public phone boxes

Exactly the same precautions are need for other pre-paid phone cards, such as those which are used in public phone boxes, to replace cash or coins.

Obviously do not make a call using your own Credit Card (which can be done in some public phone boxes, or, on some airliner flights).

All of these have unique serial numbers which can be used to link together a pattern of phone calls, so if you do choose to use one for contacting a journalist or politician or whistleblowing supervisory authorities or for any such people to contact their whistleblower contacts, then no other phone numbers such be used, even if there is still credit left on the card or the voucher. i.e. do not call your family or friends or work colleagues using the same pre-paid card card (or mobile phone) as which you use for whistleblower communications.

Using Mobile Phones and Wireless PDAs

Mobile Phones and Wireless PDAs

1. Do not use your normal mobile phone to contact a journalist or blogger from your Home Office location, or from home.

   The Cell ID of your mobile phone will pinpoint your location in Marsham Street and the time and date of your call.

   This works identically for Short Message Service text messages as well as for Voice calls.

   Such Communications Traffic Data does not require that a warrant be signed by the Home Secretary, a much more junior official has the power to do this, e.g. the Home Office Departmental Security Unit headed by Jacqueline Sharland (probably someone else nowadays, given the staff turnover within the civil service) or any middle ranking Police officer at the Superintendent level or above.

2. Do **not** store any friends or family or other business phone numbers on this disposable phone - only press or broadcast media or blogger contacts.
3. **Do store** the 24 hour contact phone numbers of some firms of solicitors experienced in human rights law - these will be useful id / when you are stopped and searched or harassed or arrested by the Police e.g.

   Kaim Todner Solicitors LLP
   City of London Offices:
   5 St. Bride Street
   LONDON
   EC4A 4AS
   Tel: 020 7353 6660 (24 hours)
   Fax: 020 7353 6661
   DX: 265 LONDON CHANCERY LANE
   www.kaimtodner.com

Bindmans LLP
275 Gray's Inn Road
London
WC1X 8QB
DX: 37904 King's Cross
Tel: +44 (0)20 7833 4433
Fax: +44 (0)20 7837 9792
Email: info@bindmans.com
Web: www.bindmans.com

4. Set a power on PIN and a Security PIN code on the phone - this may be enough to stop a Police Constable or Police Community Support Officer from rifling through your phone contacts and SMS messages illegally without a warrant, when they stop and search you, **without** reasonable cause under section 44 of the Terrorism Act 2000.
5. Make a note of the phone handset's International Mobile Equipment Identifier (IMEI), which can help you to get the phone disabled if it is lost or stolen. Most handsets will display this if the ***#06#** command is entered, and the number is on a label visible when the battery is removed.
6. For no good reason, It is often unclear what your actual phone number is when you buy a new pre-paid mobile phone or use a new SIM card. Some networks e.g. Vodafone display the phone handset number when you make a call to ***#100#**.
7. This Home Office Crime Reduction page lists the Mobile Phone Company numbers to report your stolen handset to, so that it can be quickly disabled. You do not want a thief or someone who finds your lost phone ringing up or sending or reading SMS messages from your confidential contacts on your stolen or lost mobile phone.
8. Physically destroy the phone and the Subscriber Identity Module (SIM) card once you have done your whistleblowing. Remember that your DNA and fingerprints will be on this mobile phone handset.
9. Do not be tempted to re-use the SIM in another phone or to put a fresh SIM in the old phone, unless you are confident about your ability to **illegally re-program** the International Mobile Equipment Electronic Identity (IMEI). It is possible to re-program the IMEI on many phones, often as trivially as with a Hayes AT modem style command to change a hardware register setting on a serial modem. The The Mobile Telephones (Re-programming) Act 2002 , and subsequent amendments, carry a penalty of **up to 5 years in prison**, for doing this (without the written permission of the Mobile Phone Handset Manufacturer, **not** the permission of the Mobile Phone Network Operator), or for possessing equipment and software to do this (i.e. **any** terminal / terminal emulation software and a serial computer to phone cable), or even to advertise doing this as a service.
10. Switch off BlueTooth wireless networking on your mobile phone. At the very least the device identifier can be used to remotely track your presence at a particular location. At worst, the many insecure versions of BlueTooth implementations allow a snooper to remotely look through and copy your stored contacts and photos, and perhaps even to initiate an outgoing call or a silent incoming one, thereby turning your phone into a bugging device.
11. What applies to BlueTooth, also applies to WiFi wireless connectivity, which is just starting to appear in some phones now - switch it off !.
12. A recent Court case on the USA, where the FBI bugged the mobile phone of a Mafia suspect, has re-opened the debate on whether or not some models of mobile phone e.g. the newer, more powerful ones with embedded programming languages, can be secretly turned into bugging device by the Network Operator / Law Enforcement / Intelligence agencies. Apart from the BlueTooth exploits alluded to above, this may well be true for some models of phone.

    Many modern mobile phone handsets do not really switch off when you press the "power off button". You can confirm this by setting an alarm, and then switching the handset off - many phones will "wake up" and emit an audible alarm and power up the display etc. at the programmed time. In principle, any software with access to low level functions of the phone could do this, and more, without the user being aware of it.

13. A typical bit of commercial mobile phone spyware is FlexiSpy, which can send copies of SMS messages to another phone. Supposedly, you are meant to inform the person whose phone is being bugged in this way, but since it is aimed at the jealous control freak market, this is unlikely.

    Presumably this, or customised versions of similar software, is available to the police and intelligence agencies for use in Intrusive Surveillance, when state authorised burglary of private homes or vehicles, or the use of undercover agents and infiltrators is in effect.

    However, from a whistleblower / journalist / blogger point of view, if you have already been identified to the level required to be put under this sort of surveillance, then the cat is already out of the bag, and you have been discovered.

14. You can make use of a novelty toy "flashing aerial" or other similar devices (essentially a tuned aerial coil and an LED) which light up an LED when a mobile phone is active nearby. If you have apparently switched off your phone, and the LED still flashes, or the battery gets warm, then perhaps your phone has been secretly switched on,but it is unlikely.

    If you are feeling paranoid, then either

    - Use a novelty LED mobile phone signal detector toy (might not work on all frequencies of a 3 or 4 band mobile phone or on 3G / GSM combined handsets)
    - Keep your mobile phone in an aluminium foil or other radio frequency shielded bag or container.
    - Remove the battery from your phone
    - Invest in £££ anti-bugging equipment

15. All of the above also applies to Mobile Phone SmartPhones and Personal Digital Assistants, like Blackberry or Ipaq devices.

Make sure that anyone you are meeting face to face, also obeys these tips about mobile phones.

Just in case you think this is excessive paranoia, it recently emerged that journalists in the USA and in Germany and the Netherlands, were having their phones monitored, by their national intelligence agencies, precisely to try to track down their "anonymous sources".

Why would this not happen here in the UK ?

See Computer Encryption and Mobile Phone evidence and the alleged justification for 90 days Detention Without Charge - Home Affairs Select Committee Oral Evidence 14th February 2006

Cellcrypt Tips to Stop Mobile Phone Tapping

CellCrypt, a company with a vested commercial interest in selling you some mobile phone encryption software, has nevertheless published some sensible tips aimed at businessmen:

Top Tips

Cellcrypt Tips to Stop Mobile Phone Tapping

* Never assume that voice calls are confidential (like fax or email), especially when calling internationally where some countries' phone operators have no encryption security in place at all. Check your signal, calls on 3G are more secure than 2G but often falls back to 2G when 3G is unavailable.

* Keep your phone safe and do not leave it lying around. Skilled attackers can take just a few moments to install a malicious program, compromise the security of the SIM card or install a special battery with a bug in it, all of which can later be used to help intercept calls.

* Use and protect your phone and voicemail PINs in the same way as your bankcard PIN. Never leave confidential messages in voicemails or send confidential texts. Texts in particular are easy to read on the phone and mobile phone voicemails can often be accessed from any phone with the PIN.

* Be vigilant to prevent malicious software on your phone. Be wary of texts, system messages or events on your phone that you did not ask for, initiate or expect. Turn off Bluetooth if you are not using it. Consider anti-virus / anti-malware software, and if you strongly suspect your calls are being listened to then turn off the phone when you don't need it and remove the battery as an extreme precaution.

* Use voice call encryption software on your phone to secure your sensitive calls that works worldwide and is as easy to use as making a normal phone call.

* If you have no alternative (such as using encryption software) and urgently need to discuss confidential matters over a mobile phone:

* cover your mouth so you can't be lip-read
* choose a location where you can't be overheard
* talk quietly and be brief
* use code words
* split information across different channels (e.g. refer to emails or send texts etc so information is incomplete and meaningless on its own)

Voice over IP and Communications Traffic Data Retention

Voice over IP and Communications Traffic Data Retention

Voice over Internet Protocol (VoIP) technology is what the entire telecommunications industry is moving over to. It is already available in large companies and as commercial boxed consumer products wich plug into or are part of home ADSL broadband internet connections.

1. Do remember that Voice over IP systems, like Skype, whilst they do offer privacy regarding the contents of the the conversation due to **encryption**, do **not** offer **anonymity** against Communications Traffic Data Analysis i.e. who called whom and when, which is often enough for a "whistleblower" to be identified in a "leak investigation". See the comments below.
2. Remember that VoIP operates in two modes - e.g. Skype to Skype, which is only useful if your journalist or blogger contact also uses Skype. Guido Fawkes does publish a Skype number, and Iain Dale has used Skype for video conferences etc. but does not publish his number. No major media organisations publish a Skype number, although this might well be arranged after an initial contact.
3. The second mode is Skype (or other VoIP technology) to the normal land line or mobile phone network via a gateway.

   Obviously the normal phone network part of the call suffers from all the problems mentioned above, especially to mainstream media phones which are on the "terrorist alert" watch list.

However, it is possible to use some Voice over IP systems such Vonage, to make it appear to Caller ID systems that your phone call is coming from another country. This is often enough to prevent Caller ID features on a UK land line and mobile phones from working to reveal the number you are dialling from, either through the **1471** callback feature, or on itemised phone bills of the sort which are sent to normal customers.

This is only slightly more "secure" than pre-fixing your land line or mobile phone call with **141**

Neither of these techniques are enough to protect the number you are calling from being revealed to an official UK Communications Traffic Data request, since the Networks do retain this data during at least the current billing cycle and longer. The European Union has agreed a Directive to Retain such Communications Traffic Data for at least a year, for all 450 million EU citizens, who are innocent of any crime "just in case".

~~Thankfully, has not been implemented, yet~~ Unfortunately this Mandatory Data Retention of Communications Traffic Data came into force legally in the United Kingdom, in October 2007, initially for landline telephone and mobile phone data. There is an 18 month delay before this applies to internet data.

i.e. VoIP to VoIP call Communications Traffic Data log files are not yet Retained, but VoIP to landline or mobile phone and vice versa is.

Internet connection access logs and email server logfiles, together with "Internet telephony" log files, **are** due to be retained from March 2009 onwards, for 2 years at a time, when the full implementation of the EC Directive comes into force.

Fax Machines

Fax Machines

1. From a whistleblower privacy point of view, Facsimile Machines (fax) combine the worst tracking features of land line telephones with the wear and tear induced characteristic blemishes of photocopiers and printers
2. Most models of Fax machine display or print at the bottom of each page or at least at the end of each transmission, a customisable message line which identifies the name of the company or organisation sending the fax, with its fax telephone number. If you are publishing scanned images of faxed documents, you should pay attention to the redaction or censorship of this line .
3. Since the words and numbers are user programmable (i.e. easily faked), you should not jump to immediate conclusions as to the authenticity of a faxed document, simply on the basis of this return address / return fax data
4. Since long distance phone calls , which can often be common with Faxes, cost money, there are built in electronic memory and / or printed log files available of the recent Fax transmissions ad receipts, with the identifying phone numbers and times and dates. This should be borne in mind if you do use a shared fax machine to send any whistleblowing documents to journalists or bloggers.
5. If you are sending sensitive material via fax, there is a small, but finite risk of mis-dialling, and sending it off to the wrong number entirely, which may betray a whistleblower.
6. Sometimes, a supposedly mis-dialled fax number, has in the past, been used as the "plausibly deniable" cover story, to make a deliberate leak look accidental or to add credibility to a deliberately misleading fake leak.
7. It is common practice to print or scribble a Fax Cover sheet with addressing information (and often with pre-printed Return Fax data on it. This can give clues as to authenticity of seemingly accidental fax leaks.

8. Many fax machines nowadays are effectively digital scanners (sometimes combined with photocopy and printer devices), or they eschew the process of scanning paper and simply convert , say Word document computer files into Facsimile format and then transmit them.
   Such sophisticated Fax devices may very well keep copies of the original document data files or of the image scans in their internal memory or on their hard disks, in case the fax needs to be re-transmitted.

   Fax gateways will also keep a log file of time and date when the copy was made, and details of the computer which send the fax, and, if there is some sort of electronic payment or internal accounting system, the department or people or the individual corporate client account (very common in large legal firms, for example) to which the fax costs are to be allocated..

   Even when these files are apparently deleted or overwritten, they may not have entirely disappeared, and might well be recoverable through standard computer forensic techniques. Yet another reason for whistleblowers to be extremely careful when using fax machines.

9. As with all heavily used office printing equipment, slight defects in manufacture, and heavy use, can induce characteristic blemishes on the output of a fax machine, which may provide sufficient clues to forensic investigators working for a major whistleblower leak inquiry, to track down the fax machine which was used to send whistleblowing revelations to a journalist or blogger etc.

   Consider digitally cleaning up any scratches, or other blemishes on image scans of faxed documents, before publishing them.

10. There are some **positive points** about **Fax machine telephone lines** in offices, from a whistleblower's point of view, as these can very often have special privileges compared with the other phones in the building e.g.
    - they may be made available 24 hours a day, 365 days a year, when the other phones are disabled at night or at weekends and they can usually be used to make voice calls as well as to send faxes.
    - they may also be allowed to make international calls, when the normal office phones require permission from the switchboard operator.
    - they may be the only analog POTS phone lines left working in an otherwise VoIP office, and they could be used by a laptop computer user to dial out to another office or to for a dial-up Internet Connection, in order to send an email, which does not pass through the normal office internet gateway and its logfiles.

Photocopiers, Printers and Paper

Photocopiers and Printers

The media and even bloggers need some of of credible proof about that a whistleblower has some evidence to back up their claims. This usually involves copies of internal documents.

Think very carefully before sending **original** paper documents to a journalist or politician etc. In some cases, even copies of documents which have been produced within a secretive organisation may be identifiable, and could betray the identity of the whistleblower source to leak investigators.

1. Choose your Photocopier carefully. Some of the newer, high end photocopiers, especially colour ones, have built in anti-counterfeit US currency routines in the software.

Some combined photocopiers and printers are capable of printing tiny yellow serial numbers (e.g. Canon) on each sheet or a special series of dots (e.g. Xerox DocuColor, which makes tracing which machine was used to help to "leak" a document, if the original printout or photocopy is seized, quite a bit easier.

See the Electronic Frontier Foundation's List of Printers Which Do or Do Not Display Tracking Dots

2. Many typewriters, computer printers and photocopiers do leave characteristic wear and tear imperfections on the documents they produce, which a forensics laboratory may be able to match to a machine a work or your personal machine at home, if it is ever seized as evidence in a "leak inquiry".
3. It may even be possible to **"fingerprint" blank sheets of paper**, by means of their unique surface texture properties.

   See the academic paper Fingerprinting Blank Paper Using Commodity Scanners(.pdf) by William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman and Edward W. Felten.

   Abstract

   This paper presents a novel technique for authenticating physical documents based on random, naturally occurring imperfections in paper texture. We introduce a new method for measuring the three-dimensional surface of a page using only a commodity scanner and without modifying the document in any way. From this physical feature, we generate a concise fingerprint that uniquely identifies the document. Our technique is secure against counterfeiting and robust to harsh handling; it can be used even before any content is printed on a page. It has a wide range of applications, including detecting forged currency and tickets authenticating passports, and halting counterfeit goods Document identification could also be applied maliciously to de-anonymize printed surveys and to compromise the secrecy of paper ballots.

   "Even unopened sheaves of blank printer paper might in principle have been fingerprinted at the factory."

   The is sort of technique might well be used on limited distribution copies of secret documents, which might betray the source of a whistleblower leak to investigators.

4. As noted in the comments below, many heavy duty shared network Printers and Photocopiers also have internal hard disks, especially if they are used in conjunction with Print Server devices (or effectively have these built in). These could store entire copies of documents, or logfiles of time, date and also, perhaps, the Personal Computer's IP address and/or its NetBIOS name (common in Microsoft Windows File and Printer sharing) could be logged, which might betray a whistleblower.
5. Even when these temporary buffer storage file copies of printed or scanned or faxed documents are apparently deleted or overwritten, they may not have entirely disappeared, and might well be recoverable through standard computer forensic techniques. Yet another reason for whistleblowers to be extremely careful when using shared network printers, scanners, photocopiers, fax machines, fax gateways etc.
6. Sometimes, the ability to print copies of documents to network printers or print server devices **can work in favour** of a whistleblower:
   - The fact that an important whistleblower leak document is being printed or copied or sent to a networked printer/scanner/copier/fax device, might mean that they can grab an electronic copy for themselves, or print out another physical copy when the coast is clear, without having to sneak into a colleague's or superior's office. Many of these devices have a simple worldwide web remote management interface and often still have default usernames passwords set e.g. "xerox".

- It may be possible (depending on the IT security policy, and the number of available IT support staff) to "accidentally" print or fax a copy of the whistleblower leak document to another shared printer or device on the corporate network, very often in other office or building, perhaps even internationally in foreign countries. Try the "Add a new Network printer" wizard on your Microsoft Windows PC, the print queue names very often give physical location details of exactly where the printer is located, and which may be somewhere more easily or more securely accessible by the whistleblower(s) or their friend(s).
- If you do **temporarily** attach to a **non-default** networked printer or fax etc., then remember not to leave this visible in the list of printers or faxes which are available on your PC i.e. delete this printer or fax connection icon in the Printer Control Panel settings, after you have finished with it.
- Modern photocopier / scanner units can have quite sophisticated "security" and networking features, but unless these have been properly configured, integrated and tested by an organisation's IT security team, then these extra features may actually be a source of "whistleblower leaks" or espionage targets. e.g. the "security" features like digital watermarking, encryption, Single Sign On (almost certainly with an audit trail log file) etc. offered by, for example, Canon's mid range Office products, hint at what an unsecured photocopier / scanner / printer connected to a network is capable of:

  Canon iR6880Ci photocopier brochure

  [...]

  Prioritise your work

  You can easily prioritise your workload with the new Print Job feature. Jobs can be viewed and repositioned within the print queue whenever your needs are pressing. Secure and encrypted jobs are hidden by an asterix and, by using Single Sign On (SSO), only your jobs are viewable when you access the device.

  Guarantee secure communication with the iR5880/6880C/Ci:

  Document security - hold confidential documents in password protected secure mailboxes, encrypt scanned documents before sending, or embed a secure watermark to prevent unrestricted copying of confidential documents

  Device security - Ensure only those authorised to use the iR5880/6880C/Ci can access using passwords, your company's network log-in, or even fingerprint authentication. For further peace of mind, hard disks can be erased or encrypted and job logs can be concealed.

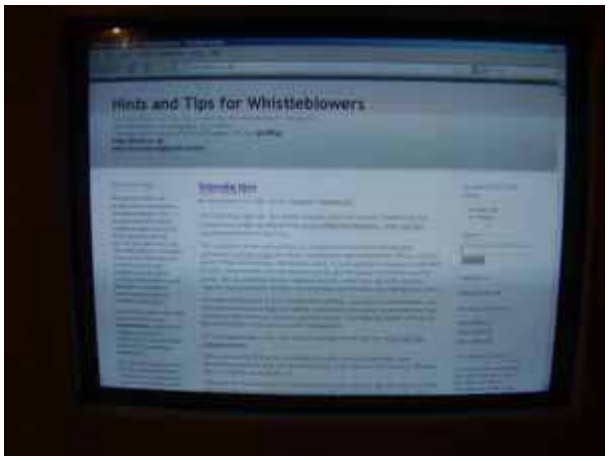
Shift PrtScr - Screen Dumps and photos of Computer Screens

- One of the traditional "old school" methods of leaks from Police, Government Departments, Banks etc. which used heavily restricted mainframe computer terminals, was to do a "screen dump" to a locally attached (cheap and slow) printer, which would not show up in any network printer queues. Most dedicated terminals have been replaced these days by Terminal Emulation software running on a Personal Computer, but the same trick can often be used, even when the user is not allowed by the heavily audited mainframe legacy or core business system to save files or print

copies, they may simply be able to take Windows (or Terminal Emulator scroll history) "screen captures" or "screen dumps" which they can print locally or save as files to removable media like USB memory devices etc.

N.B. See also the sections on Photocopiers, Printers and Paper, Electronic Document Files and , CD-ROMs and DVDs and USB flash memory media and File Deletions

- See the Windows PrtScr Key (sometimes labelled Print). The keyboard combination of the **Ctrl** and **PrtSc** keys together will capture, into the common Windows Cut and Paste buffer, a (.BMP) image of your entire Windows screen. The combination **Alt** and **PrtSc** together will do the same for the individual Window which you are focussed on e.g. a Terminal Emulator or Web Browser window. The contents of the Windows Cut and Paste buffer can then be dumped into the graphics capable Write accessory or any Microsoft Office application like Word etc. with **Shift** and **Insert** together (or **Right Mouse button** / **Paste**)
- It may be necessary to use several screen captures to copy a scrollable page or list from a computer screen.
- In some circumstances, where the system does not have any (whistleblower safe) printers etc. it may be possible to **photograph a computer screen** displaying whistleblower information, using a digital camera or mobile phone camera.



- Several photos might be needed of the same screen, if the camera speed settings cannot be adjusted, and "video synch" lines" obscure some or all of the monitor screen. Flat panel computer or laptop displays should be easier to photograph.
- Remember to **turn off the auto flash** setting on your camera or mobile phone, if this might arouse suspicion amongst co-workers or CCTV camera operators etc.

Electronic Document Files

Electronic Document Files

Many electronic file formats contain extra information about the document itself, regardless of what the contents of the document actually are. This metadata usually gives clues as to the physical hardware and possibly the actual user account information of the creator or editors of a document,

together with time / date stamps etc, any of which may be **hazardous to the anonymity of a whistleblower**.

On the other hand, this metadata embedded within a leaked document may provide the **strongest clues as to its authenticity.**

1. Adobe .pdf documents have been published online, where some of the personal details e,g, email addresses have been "blacked out" using Adobe .pdf software , which has effectively simply put an extra layer on top of the supposedly censored words. Simply copying and pasting into say Windows Notepad or Wordpad or Word etc. has revealed the hidden data.

   Anybody publishing such stuff online needs to be aware of this, to protect their Home Office or other sources.

2. See this Adobe Technical Note:Technical Redaction of Confidential Information in Electronic Documents - How to safely remove sensitive information from Microsoft Word documents and PDF Documents Using Adobe Acrobat (.pdf) (or from our local mirror copy here at ht4w)
3. Similarly Adobe .pdf documents or Microsoft Word documents, Excel spreadsheets etc. may well have Meta information (see the Document Properties) showing the author of the leaked document (which may in turn lead back to the "leak source").
4. Microsoft Word Documents, especially draft documents worked on by several people, often have the Version feature enabled. Sometimes examining the changes made to a document, and by whom gives extra clues about policies or coverups etc.

   The same feature on a whistleblower's own computer, could, of course betray their identity, by adding their default name properties to any document which they edit or view, before passing it on.

5. Older versions of Microsoft Word (and other Office products like Excel or PowerPoint) can also betray the MAC Address of the Ethernet card of the computer on which a document was created or edited on, as part of the Global Unique ID data, embedded in the document. Most people will not have changed the MAC addresses of their computers (often possible through software), and there are likely to be inventory records or network logfiles which will pin point which MAC address belongs to which computer either at work or at home.
6. Microsoft do now make available some tools to remove such GUID and other hidden meta data, versions, comments etc. from final published Microsoft Office products. e.g. the Microsoft Office 2003/XP Remove Hidden Data Add-in which removes most of, but not quite all of the Hidden File Data in Microsoft Word, Excel, and PowerPoint files. N.B. this does **not** work on Office 2007 files, but there seem to be built in Document Inspector settings, which do this as standard, but not by default.

   Types of data this add-in can remove

   The following types of data are removed automatically.

   * Comments.
   * Previous authors and editors.
   * User name.
   * Personal summary information.
   * Revision marks. The tool accepts all revisions specified in the document. As a result, the contents of the document will correspond to the Final Showing Markup view on the Reviewing toolbar.
   * Deleted text. This data is removed automatically.

* Versions.
* VB Macros. Descriptions and comments are removed from the modules.
* The ID number used to identify your document for the purpose of merging changes back into the original document.
* Routing slips.
* E-mail headers.
* Scenario comments.
* Unique identifiers (Office 97 documents only).

Note The Remove Hidden Data tool also turns on the Remove Personal Information feature. For more information on this feature, please search for "Remove Personal Information" in the application Help.

7. The US National Security Agency has published a technical report: Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF (.pdf) - (or from our I733-028R-2008.pdf local ht4w copy)
8. See also Microsoft's Knowledge Base article KB223396 pointing to other articles about meta data in various Microsoft Office products: How to minimize metadata in Office documents

Obviously any journalist or blogger should double check that what they make available online does not contain identifiable clues to their anonymous sources, not just on the face of the published document, but within any "track changes" previous versions of a document, or document template as well.

Track Changes and Versions

1. Remember that Microsoft Word has a "track changes" facility, which is useful when different versions of a document are written, edited or approved by more than one person. Several politically embarrassing Government leaks have happened because previously edited versions of words or paragraphs have been revealed by the public simply turning on the "show changes" option when they read it in Microsoft Word.

   The Liberal Democrat blog Home Office Watch reports on how the extremely controversial secret policy document regarding plans for "Big Brother" surveillance of millions of innocent people was revealed because **someone forgot to turn off "track changes"**.

   As more journalists and political activists are becoming familiar with this feature or vulnerability, this may perhaps sometimes be a useful **covert channel** for information to be leaked to the media and the public, with a certain amount of "plausible deniability" for insider whistleblowers i.e. one document is effectively hidden within another, to a casual observer.

2. The more recent versions Microsoft Word i.e. 2003, 2007 have a couple of Security / Privacy options which are worth enabling under the **Tools / Options / Security** menu.
   - Remove personal information from file properties on save (**off** by default)
   - Warn before printing, saving or sending a file that contains tracked changes or comments (**off** by default)
   - Store a random number to improve merge accuracy (**on** by default) - supposedly a harmless random number, but worth switching off if you are not merging documents with anything else.
   - Make hidden markup visible when opening or saving (**on** by default) - worth keeping on to let you check that you have successfully erased identifying personal data if necessary.

   N.B. "Authoring references not entered by the application are not removed automatically. For instance, those references entered through the use of field codes are not removed or changed.

Or, if hidden text was used to tag a line, and the author of the hidden text embedded his or her initials or name in the hidden text, this reference is not removed because it is not an identified author reference."

Examples of Inept "Redaction" or Censorship

1. Sometimes digital files simply copy and magnify the errors which are the result of people being under a time pressure deadline. See the inept redaction / censorship with a marker pen of a legal Exhibit document in the Bank Julius Baer versus Wikileaks court case in February 2008. The plaintiff's lawyers took a digital screendump of a web page, which they then printed out and tried to hide the name of one of their clients former customers, by using a black marker pen, and the digitally scanning the result and submitting it electronically to the Court, as an Adobe .pdf document. Apart from failing to redact or censor the postal address of the customer and the name of the customer in the heading of a page (printed in the largest typeface used in the document), they also failed to cover all the descending tails of the lower case letters in the name, which could have led to some intelligent guesswork. By digitally zooming in on the .pdf image scan, the name could be read through the fading marker pen ink overlay.

   See Lavely & Singer demonstrate how not to protect the confidentiality of customers of Bank Julius Baer

2. Sometimes (.pdf) files have been "Redacted" or Censored by using the Drawing facility within the software to "paint" thick black lines over the text as an overlay. This has led to several "whistleblower leaks" of the hidden data, through the simple technique of copy and pasting the text out of the (.pdf) viewer software into a another application programme such as a text editor or word processor, which has then revealed the underlying words which have supposedly been hidden. e.g. the failed attempt to hide the IP Addresses of military and government computers, in a (.pdf) copy of a US Grand Jury indictment against the alleged UK computer hacker Gary McKinnon
3. Sometimes the encryption and "protection" features used to hide information in an Adobe (.pdf) file can be overcome through password guessing etc. e.g. the Wikileaks.org publication of an unredacted version of South African Competition Commission's final Report on Banking, 12 Dec 2008

Document File MetaData

1. The ExifTool Perl scripts or Windows binary executable which reads the meta data of image files, also displays it for Microsoft Word .doc, Excel .xls, Powerpoint .pps and Adobe .pdf files etc. as well. - see the Photo Image Files section
2. You can examine (but not change or delete) such photo or document image metadata via this website, which is powered by the ExifTool perl script software: Jeffrey's Exif Viewer

Remember that sometimes a whistleblower or journalist or blogger needs to read and understand this sort of hidden meta data or document change history, to help to determine if the leaked document is genuine..

If the leaked document has not been edited on a computer which is linked in anyway to the whistleblower, then sometimes, the hidden meta data and "track changes" edits are in fact the **main point of the whistleblower leak**, perhaps showing evidence of a last minute reversal of Government or Corporate policy, or the censorship of independent expert advice, or even the outright fabrication of "facts" by political spin doctors in the final version of a document etc.

Photo Image Files

Photo Image Files

1. Photo images. Your source or the "anonymous" publisher of a leaked document online may use a Scanner, but they may, nowadays use a Digital Camera.

   There is often camera make / model identifying **metadata** embedded in the raw digital images taken by many types of Digital Camera. These may be used as "evidence" if your Digital Camera is seized during a "leak inquiry" investigation.

   There is even facility for Global Positioning Satellite **latitude and longitude data** (likely to become increasingly common with mobile phone camera pictures) to be stored within this metadata, and **camera specific serial numbers**, which, if cross referenced with purchase or repair or warranty registration records, may provide clues or evidence as to the identity of your confidential source.

   See this report in The Times (19th July 2007) about the embedded EXIF data which reveals the Camera Model and Serial Number, which may be of use to copyright lawyers, in tracing the photographer who allegedly leaked images onto the internet, of the then as yet unpublished popular novel *Harry Potter and the Deathly Hallows*, the final book in the immensely popular and profitable series by J.K.Rowling.

2. There is an excellent free Perl module and a Windows executable command line tool called ExifTool, which displays, and can selectively edit, most of this metadata which is encoded according to the industry standard Exchangeable File Image Format (Exif)
3. You can examine (but not change or delete) such photo image metadata via this website, which is powered by the ExifTool perl script software: Jeffrey's Exif Viewer
4. Standard image editing software such as Adobe PhotoShop can preserve the original metadata, which is useful for keen photographers, but not so good for preserving the anonymity of your anonymous sources.

   Very often using File Save As within the image editor, and saving to a different filename from the original automatically digital camera name and numbered images, reduces the amount of metadata to an acceptable level.

5. Another freely available command line tool, for both Windows and Linux, (which does not require Perl to be installed) is jhead. Whilst not as comprehensive in displaying all the EXIF data, as ExifTool (which also now has a Windows executable binary version), and restricted only to .jpg files (the most common digital camera output), it does provide the ability to edit comments (e.g. to put in your own copyright notice) and to delete all the potentially whistleblower source betraying EXIF data.
6. You may wish to blank out or censor items in .jpg or .gif or .bmp graphics image.

   Again, there is a temptation by the uninitiated to use, say, a PhotoShop pixellation or motion blur special effect filter. Remember, that these standard filters effects **can often be reversed.** e.g. as Interpol has shown with the enhanced version of the reversible PhotoShop Twirl plug-in effect used to try to identify a suspected child rapist

   Since Digital Camera images and Scans of documents are usually much too large for web pages, you might want to reduce the number of colours and probably the size of the images, before publishing them as thumbnails and even as larger images on a blog or website.

Remember to apply your PhotoShop pixellation etc. **after** reducing the image size and number of colours, i.e. after you have thrown away some of the identifying data, so as to reduce the chances of the filter effects being reversed.

7. The jhead documentation and program options remind us that many digital cameras embed a small, up to 10Kb thumbnail image in the file, used by the camera display itself, or external software, to show for thumbnail gallery views of a set of photos.

   If you are digitally manipulating the main image e.g. to pixellate out a face or a location specific sign, a vehicle number plate, or to redact an email address or telephone number etc., then the thumbnail also might need to be re-generated from the modified main image using jhead, or else the thumbnail should be deleted.

8. EXIF metadatais not the only way of forensically linking a digital image from a whistleblower source to other digital images which may be more easily traced to the source camera or scanner.

   Cameras or Scanners introduce potentially characteristic non-random background noise into the images which they produce, as a combination of individual wear and tear patterns and the variations within the manufacturing tolerances, and small errors, such as faulty pixels on the Charge Coupled Device electronic chip, of any particular device.

   Professor Jessica Fridrich, of the Thomas J. Watson (founder of IBM) School of Engineering and Applied Science at Binhampton Uniiversity in the State of New York, has published Camera Identification From Printed Images (.pdf) academic research and software which can statistically compare such background noise patterns (Photo-Response Non-Uniformity) , and match a series of digital photos together as having been made by the same digital camera or mobile phone camera or scanning device. If some of the photos are easily identifiable, due to their content or metadata, e.g. on a public photo sharing website like Flickr.com, where family album or holiday snaps might betray the identity of the whistleblower, if he or she uses the same equipment for their confidential or leaked photos.

   See the step by step guide and comments - Avoiding Camera Noise Signatures

CD-ROMs and DVDs and USB flash memory media

CD-ROMs and DVDs and USB flash memory media

If your whistleblowing documents are too large to fit onto a floppy disk e.g. they contain lots of digital photos or video or audio clips etc. then you might be tempted to write them to a CD-ROM or DVD disc or USB flash memory media (USB memory sticks, MP3 players, digital camera or mobile phone removable memory etc.), which can be ok, if you remember that

1. CD-ROM and DVD discs are excellent for taking fingerprint impressions and DNA samples, which may betray the identity of a whistleblower or a courier who has physically handled them or their plastic packaging.
2. Most CDROM or DVD writer equipment sold since 1995 contains an industry standard mandated (.pdf) Serial Number called a **Recorder Identification Code**, which is in three parts, denoting the Manufacturer, the Model, and a 20bit Serial Number uniquely allocated to each recorder. The RID was introduced as a sop the powerful music and film industry lobbyists seeking to commercially exploit copyrighted material.

   This RID is burnt into each CDROM or DVD disc which the writer copies, This serial number may

provide evidence matching a whistleblower's home or office computer to a leaked copy of documents or photos or videos etc on a seized or intercepted CDROM or DVD.

3. Given the difficulty, or, with some of the technologies, virtual impossibility short of physical destruction of **securely erasing** or genuinely overwriting data files, a whistleblower should **use a fresh "virgin" blank** or at least a low level formatted floppy disc, CD-ROM, DVD or flash memory device, on which to copy their whistleblowing leak documents or other video or audio data files, even if these files are themselves protected with strong encryption or other steganographic techniques which embed the data hidden within, say, graphics or music files.

USB keys and SmartMedia

These are useful to spies or to whistleblowers, for smuggling out electronic copies of documents. Given the size of the memory capacity these days, which is often larger than hard disks of only a few years ago, a very large amount of data can be carried.

They are small and easy to hide, and can also legitimately be hidden in mobile phones, digital cameras or MP3 music players etc.

1. Some Government Departments e.g. the UK Ministry of Defence do tend to use modified operating systems software which controls access to floppy disk drives, CDROM, DVD or USB devices, either totally preventing their use, or logging all such uses to a central audit server.

   We suspect that not every desktop PC in the Home Office is protected in this way.

2. The use of USB memory or other USB connected devices e.g. an Apple iPod or other MP3 player, leaves a trail on the Windows computer to which it was attached e.g. you can see a list of such devices which have been connected successfully to a particular PC running WIndows XP via the Registry Key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBTOR**.
3. Some US government departments and agencies, like the Department of Homeland Security (DHS), use the National Security Agency (NSA) developed **USBDetect** scanning software, (see page 13 of this 2008 report Review of DHS Security Controls for Portable Storage Devices (.pdf) which centrally audits the Registries of connected Windows computers, looking for the Registry traces of USB devices. Such software can only detect "policy violations" and it "does not identify if USB devices are currently connected, nor if any sensitive information was copied"
4. If you have permission to access the Registry on the Computer, you can, of course delete the entries generated by your use of a particular USB device. However, most corporate or government PCs will have this sort of access restricted to privileged systems administrators only, so a whistleblower should make sure that they are not using an unusual brand of USB device which stands out from the crowd of entries which might plausibly be found in that environment.
5. USB memory devices (and also CDROM or DVD devices) **leave traces of their use in the Windows Registry**. It is even possible to correlate the amount of data transferred with the time taken to do it in, to narrow down or even specifically identify, the make and model of USB device used.

   This may be enough of a clue to "leak investigators", although this experimental technique is certainly not yet established in Court for legal evidential purposes.

   See this New Scientist article

   USB fingerprints identify 'pod slurping' data thieves

   * 16 February 2010 by Paul Marks

[...]

Vasilios Katos and Theodoros Kavallaris at the Democritus University of Thrace in Komotini, Greece, have been testing every make and model of USB stick and iPod/iPhone. They have discovered that each one has a distinctive transfer rate when copying data from a PC's hard drive (Computers and Security, DOI: 10.1016/j.cose.2010.01.002). This is due to the differences in the microcircuitry and components that go into making each type of device.

They are able to find out if files have been copied by consulting the Windows registry, which records the make and model of every USB device plugged into that computer with a time stamp. The pair then check all document folders for any files that were accessed shortly after the USB device was plugged in - the computer registry counts copying as file access.

When they find a folder they suspect has been copied, they list the times the files within it were accessed. If the total time it took to access all the files matches the transfer rate of a particular USB stick or iPod plugged into the PC at that point, then it is fair to assume a pod-slurping attack has taken place.

Kavallaris is writing a program to automate the process of trawling the Windows registry to work out which files have been copied to a USB stick.

[...]

6.
7. Deliberately "erasing" the "whistleblower files" stored on USB memory sticks, Digital Camera or MP3 music player memory devices, which can then be recovered with File recovery utilities (e.g. those designed to recover accidentally erased Digital Camera images , such as PhotoRescue) once the whistleblower is in a safe place, may well be enough to let a whistleblower smuggle out copies of sensitive documents past cursory security checkpoints,
8. Depending on the operating system and the particular settings on your PC, USB memory devices may have a **local Trash or Trashcan folder on the USB device** itself, in addition to the main one on the computer Desktop. Sometimes this is a **Hidden** folder or directory on the USB memory device, e.g. Apple Mac OS X and Ubuntu Linux.
9. However, if you are caught with a USB key or MP3 player or SmartMedia memory stick or card, which uses Flash Memory, they are nigh on impossible to securely erase electronically, and there is a good chance that data on them, even if "deleted" can be forensically recovered.
10. It is even possible for USB Flash memory data to eventually be permanently "burned in" to memory cells, which cannot then be erased. There are also "wear leveling" and "block write" algorithms, which may fail to physically overwrite crucial data, which you are trying to erase.Therefore do **not** store your PGP Private Keyring or other vital data, on unencrypted USB Flash memory. See the Wikipedia article on Flash Memory
11. Older operating systems like Windows 98 or WIndows 2000 require that you **Stop** the USB memory device before you physically remove it, otherwise the latest data which you have tried to save / overwrite or erase may not actually get written from the memory buffers into the Flash Memory cells, since this tends to use "block writes", rather than random access writes, to the individual memory cell locations. Obviously this can also lead to supposedly erased or overwritten or amended files not being updated properly, if the USB Flash Memory device is simply yanked out of the slot in a hurry.
12. We hope to publish information on the levels of risk for (in)secure data erase behavior of different types of USB or other SmartMedia. - see the File Deletion hints and tips section.

13. Obviously, sometimes the all too common failures with CDROM, DVD and USB data handling security, by government or corporate employees, is itself the actual source material for whistleblower leaks.

The Daily Telegraph reports that the former MI6 employee Daniel Houghton, who is being tried under the Theft Act and the Official Secrets Act, for **ineptly** trying to sell alleged MI6 and MI5 "intelligence gathering techniques" secrets to undercover UK counter intelligence agents, used this USB technology to smuggle out and store the alleged top secret and secret documents:

Spycatchers trap MI6 man 'trying to sell secrets'

Daniel Houghton, 25, was caught in a sting operation after allegedly approaching a foreign intelligence agency offering to sell them information he had collected while working for the Secret Intelligence Service, known as MI6.

The files, which belonged to the domestic security service MI5, allegedly related to the capabilities of the security and intelligence services and the techniques they have developed to gather intelligence, sources said, and were labeled "top secret" and "secret."

Houghton, who worked for MI6 between September 2007 and May 2009, allegedly telephoned the foreign intelligence service three months after leaving MI6 to try and arrange a deal.

But undercover MI5 officers, known as "spy catchers", met him in February to view the material on his laptop and allegedly negotiated a price of £900,000, while recording the meeting with hidden listening devices.

Houghton allegedly told them he had downloaded the information onto a number of CDs and DVD disks which he then copied onto a secure digital memory card of the type used in cameras.

He also allegedly told the undercover MI5 officers that he had **copied material onto a second memory card** which he had hidden at his mother's home in Devon.

They arranged to meet him again at a central London hotel where he allegedly showed them the material on a laptop and then handed over **two memory cards and a computer hard drive**.

Sources said he was allowed to leave the hotel room with £900,000 in a suitcase before he was arrested as he waited for a hotel lift by plain clothes officers from the Metropolitan Police Counter Terrorism Command.

[...]

Presumably this smuggling out and storage of the sensitive secret electronic files on to USB SD card camera memory went undetected, until his inept, amateur attempt to sell the information.

Hard disk and USB Memory device Encryption

We will be expanding this section soon, with a Guide to using TrueCrypt

1. PGP also does Disk Volume Encryption, which may be of use to a whistleblower's home PC.

2. There are other Disk Volume Encryption systems available, such as TrueCrypt, which is Open Source and free, and also available for the current versions of Microsoft Windows. This offers potentially two (or more) pass phrases, one of which will decrypt to one set of files, which could be innocent but private data e.g. bank account details. This pass phrase could be revealed to "leak investigators" if necessary.

   However, a second, "hidden volume" with its own separate pass phrase can be incorporated within an encrypted volume (which looks just like a big block of seemingly random data), which is where sensitive or illegal material can be stored, with quite a high degree of plausible deniability.

   Whether you can ever get your interrogators to actually believe that you have really given them **all** the pass phrases, to all the possible hidden encrypted volumes, is a risk assessment you have to make, depending on exactly what "secrets" you are leaking as a whistleblower.

tor2web.org/

File deletions

File deletions

1. Hiding incriminating evidence (either of your "leak" or of the actual malpractice, incompetence, corruption or other criminality which you are trying to draw public attention to) is not as simple as hitting the delete key on your computer keyboard.

   At a simple level, some people forget that file deletions can be recovered from the "waste basket", and with a hex editor or recovery utilities, many files can be "undeleted", simply by changing the first character of the deleted file name, provided that it has not yet been overwritten.

2. The popularity of Digital Cameras, has lead to the availability of lots of free or cheap Digital Photo file recovery tools which work in this way, which usually succeed very well in "un-deleting" photograph image files which have been accidentally "erased" on Flash Memory or other Smart Media or which have become otherwise corrupted e.g. Photorescue etc.

   What works for (,jpg) image files also works for Microsoft Word (.doc) or Adobe (.pdf) whistleblower files etc.

3. Remember to hide your personal details when Purchasing such software online, or Registering for a time or use limited "free" demonstration version of such software - obviously do not do this from work !
4. Deliberately "erasing" the "whistleblower files" stored on USB memory sticks, Digital Camera or MP3 music player memory devices, may well be enough to let a whistleblower smuggle out copies of sensitive documents past cursory security checkpoints, which can then be recovered once the whistleblower is in a safe place.
5. Deleting corporate emails e.g. Microsoft Exchange is not a simple matter either. Very often deleted emails can be simply recovered from the "wastebasket" deleted folder. Anything that has remained on the system for more than a few hours, is likely to have been backed up to other backup storage media, and so may also be recoverable during a "leak inquiry" investigation.
6. Make sure that you delete the Browser History and Temporary Files (Tools / Internet Options / Delete Files / Delete all off-line content and Tools / Internet Options / Clear History in the Microsoft Internet Explorer web browser) - it is not just your internet browsing which is monitored, it is also your **intranet** web browsing, search engine queries and document downloads, which are potentially monitored.

Securely erasing Hard Disks

1. Sometimes the actual source of "whistleblower leaks" and Security / Privacy breaches, is the incompetent (or penny pinching) attitude of government or corporate employees, who fail to securely dispose of old computers and hard disks etc. or who lose them or allow them to be stolen.
2. "Secure" deletion utilities repeatedly write binary patterns over the deleted filespace several times, to try to frustrate even the more sophisticated magnetic disk surface reading equipment, which can pick up the "shadows" of previous patterns of zeros and ones. However this does take quite a long time to do thoroughly.

   Even multiple deletion passes do not really obscure the magnetic track edge information, which can sometimes be used to re-construct the patterns of zeros and ones on a magnetic data storage hard disk.

3. Magnetic de-gaussing of hard disks is also no longer guaranteed, especially if done in a hurry, as high density storage technologies such as perpendicular recording (i.e. vertically through the thickness of a magnetic coating, not just horizontally on the surface) or magneto-optical techniques, involving lasers to thermally temporarily lower the magnetic coercivity, come into use.
4. There are also laptop / notebook / mobile phone computer hard disk drives which have large Flash Memory buffers which will contain a large amount of recent data and which will not be affected by magnetic de-gaussing.
5. Even physical destruction of hard disks can leave traces of important data still readable, as the recording density of the technology keeps increasing. i.e. even a small fragment of a modern hard disk potentially now contains quite a lot of data.
6. Many modern ATA / IDE hard disks (usually those with a capacity larger than 15 GB) do actually incorporate a Secure Erase function, called the **ATA Security Feature Set,** built into the hard disk electronics

   Some free software (HDDErase.exe) to use this feature, and plenty of other useful advice is available from the Secure Erase project, originally sponsored by the US National Security Agency, headed by one of the pioneers of hard disk technology, Dr. Gordon F. Hughes, at the Center for Magnetic Recording Research (CMRR), at the University of California San Diego (UCSD)..

7. Whole Disk or at least Whole Volume Encryption (e.g. using TrueCrypt strong encryption software) is a viable option to frustrate data thieves, computer forensics investigators and whistleblowers, provided that the actual de-cryption pass phrases are held or stored securely e.g. not written down on a bit of paper kept in the same laptop computer bag as the hardware it is supposed to protect, so that they can both be lost or stolen together.

Physical Meetings

Physical Meetings

"But why did we not breakfast at the Parpaillot?"

"Because **we have very important matters to communicate to one another**, and it was impossible to talk five minutes in that inn without being annoyed by all those importunate fellows, who keep coming in, saluting you, and addressing you. Here at least," said Athos, pointing to the bastion, "they will not come and disturb us."

"It appears to me," said d'Artagnan, with that prudence which allied itself in him so naturally with excessive bravery, "that we could have found some retired place on the downs or the seashore."

"**Where we should have been seen all four conferring together, so that at the end of a quarter of an hour the cardinal would have been informed by his spies that we were holding a council**."

"Yes," said Aramis, "Athos is right: *animadvertuntur in desertis*."

"A desert would not have been amiss," said Porthos; "but it behooved us to find it."

"**There is no desert where a bird cannot pass over one's head, where a fish cannot leap out of the water, where a rabbit cannot come out of its burrow, and I believe that bird, fish, and rabbit each becomes a spy of the cardinal**. [...]"

Chapter 46, The Bastion Saint-Gervais, *The Three Musketeers*, by Alexandre Dumas, 1844 - text available online via Project Gutenberg

It may sometimes be possible to be a whistleblower without physically meeting a journalist or blogger or anonymous source. Often this is unavoidable, if the story is to be made public.

1. If you decide to meet with an alleged "journalist" or blogger (who may not always be who they claim to be), or if a journalist or blogger decides to meet with an "anonymous source" (who also might not be who they claim to be), then you should switch off your mobile phones, since the proximity of two mobile phones in the same approximate area, at the same time, is something which can be data mined from the Call Data Records, even if no phone conversations have taken place. Typically a mobile phone will handshake with the strongest Cell Base Station transmitter every 6 to 10 minutes, and this all gets logged, all of the time.
2. Similarly choosing a suitable location for a meeting needs some care. Nipping down to a local pub near to to the Marsham Street Home Office complex may be convenient, but your presence and that of the journalist etc. is likely to be noted by some of your work colleagues.
3. There are now vast numbers of CCTV camera in UK cities, especially in London, none of which are of much use in preventing or deterring crimes, and very few of which are monitored by humans in real time. However, the sheer numbers of cameras and recording equipment does pose a threat to whistleblower anonymity.

   Luckily, the vague 1980's planning rules apply, which treat CCTV cameras like external advertising signs etc. on buildings, into which, inevitably, people could bang their heads, so almost all CCTV cameras are mounted more than 2.5 metres above the ground. They therefore rarely get a clear picture of anyone's face, if they are wearing a hat or a hoodie. or a scarf etc. .

4. If you travel by public transport in London, to get to your physical meeting with whistleblowers, journalists, campaign activists or bloggers etc.bear in mind the tracking capabilities of the Transport for London Oyster SmartCard. This stores the pttern of your last 20 or so journeys on the Card itself, with a 6 month history at least , being kept on the central computer system. If you have registered the card or have paid for it with a credit card etc., then it could easily betray your identity, especially if your use of it on the tube or Bus is also caught on CCTV camera.
5. If you drive a vehicle in London, remember that there is the City of London "ring of steel", the Central Congestion Charge Zone, the Westward Expansion Congestion Charge Zone and the wider London Low Emissions Zone, all of which are enforced using Automatic Number Plate recognition CCTV cameras. Apart from the City of London cameras, the rest are all linked to Transport for London central control rooms. Since July 2007, all of this CCTV camera and the Automatic Number Plate Recognition, and lookups to the DVLA, and mobile phone / credit card payments are all being slurped, "in Bulk, in Real Time" to some secret Data Warehousing project run by the

Metropolitan Police Service, supposedly for "national security", all of which has been made exempt from the Data Protection Act, by Ministerial fiat. If you are in a vehicle, it is certainly worth trying to avoid crossing any of the ANPR Zone boundaries on your way **to or from** the meeting

See Home Secretary Jacqui Smith cripples the Data Protection Act regarding the London Congestion Charge ANPR Mass Surveillance scheme

This vast amount of data,**on millions of innocent people** and powerful computer analytical tools could easily be turned away from its supposed task of hunting for suspicious terrorist movement patterns, and could be asked to help to track down potential Government whistleblowers and their journalistic or other contacts, since "national security" can easily be invoked, even when the only secrets being leaked are political coverups, incompetence or corruption.

6. Remember the Cold War Moscow Rules from espionage fiction.
7. Some idea of the precautions necessary for making sure that you have not been followed to clandestine physical meetings, on foot or by car, can be gleaned from this re-print of advice and techniques given to ANC / Communist activists under the South African apartheid regime in the 1980's - How to Master Secret Work . This is even more difficult now with CCTV cameras, Automatic Number Plate Recognition and mobile phones. The common use of mobile phone and MP3 music players means that people wearing earpieces and apparently talking to themselves in the street is no longer as suspicious as it used to be.
8. The more up to date A Practical Security Handbook for Activists and Campaigns (v 2.6) (.doc - 62 pages), by experienced UK direct action political activists (www.activistsecurity.org). is full of practical advice, on many of the topics in this blog, including physical meetings, surveillance and mobile phones.
9. See also the section on Covert Channel Signals for Meetings or Dead Letter Drops for some ideas about Covert Channel Signals, which might also be useful for arranging an urgent secret physical meeting between a whistleblower source and their journalist or activist or other contacts, without arousing suspicion

GPS satnavs and interactive web maps

1. If you use a motor vehicle (private or commercial) to travel to your meeting place, remember that the increasingly common Global Positioning Satellite in-vehicle navigation units ("**satnavs**") are electronic devices just like mobile phones etc, which contain flash memory which can be read under forensic examination, even when the data is nominally erased. This could betray your movement patterns and give intelligence about, or hard evidence of the time and location of your secret meeting.
2. Some units also synchronise with your mobile phone, via BlueTooth, in order to download the latest traffic information or map updates etc, and that could leave a trace of whose mobile phone was present in the vehicle at a particular time and location. - See this New Scientist article Why satnavs are a detective's best friend.
3. One of the features of such satnav devices is the convenience of setting up pre-set destinations e.g. "Home", something which can be exploited e.g. there have been warnings from the Police about gangs of thieves, who have burgled an obviously empty property, after discovering its location (and route directions) from a stolen satnav. Such pre-set navigation data could also be used by snoopers to track your movements retroactively, and possibly therby betray your meetings with anonymous sources or friends. Sometimes it may be worthwhile not to store very precise navigation endpoint data in such satnav devices e.g. instead of the precise post code or ordnance survey map coordinates or latitude and longitude for "Home" or for "Secret Meeting Location", you could only store the nearest landmark which puts you on the same page of the map e.g. a local railway or bus station or tourist attraction.
4. Further research needs to be done, on particular models of satnav devices (including **mobile phones with built in GPS chips**), to determine if the device actually keeps a logfile of the

searches for particular locations, e.g. the file names names and last displayed time and date data, of the individual graphics files used to display a particular grid square on the interactive map display, or if such data is only held transiently in the memory of the device.

Such graphical file data is defiantly logged by online web sites which offer interactive maps, so you need to take anonymous web browsing precautions (e.g. clearing the browsing history and cached data, using Tor etc.) if you are using such general mapping (e.g. Google Maps, Streetmap.co.uk, Multimap etc) or public or commercial transport time table web sites (e.g. Transport for London, Tube, Rail or Bus timetable systems, RAC Routefinder etc.) to plan a route to a secret meeting.

N.B. trying to erase such data from, for example, an Apple iPhone's Safari web browser, which takes snapshot images of the web pages which have been visited, as part of the clever / fiddly touch screen system, is almost impossible, short of re-flashing the whole device (this is a separate issue from the more general one of the easy recoverability of a a lot of supposedly erased data on flash memory devices).

Dead Letter Drops and Geo Caches

For Whistleblowers, unlike a Spy or Secret Agent, the use of Dead Drops / Dead Letter Drops or Caches, is unlikely to be a regular occurrence, and may only need to be used once, in order to pass on some actual physical evidence which supports a whistlelblower's claims.

However, pretty much the same precautions apply, both in choosing an appropriate location for the drop, signaling when and where there is something to be picked up, and taking anti-forensic precautions, in case the physical package is lost or intercepted, whilst preserving it from damage by the weather or even by wild animals etc.

You may be able to disguise your real "whistleblower" Dead Drop activity if it is near an "innocent" GeoCache site.

1. Wikipedia article on Dead Drops / Dead Letter Drops etc.
2. Wikipedia article on Geo Caching
3. Magnetic Geo Cache tips

    Location

    With a magnetic nano cache you can really have some fun when deciding on where to put it. It obviously needs something ferrous to stick to and because of its magnet, you can put it in places where regular cache container wouldn't be suitable.

    Try placing the cache underneath something such as a park bench or bridge support. You can be as devious as you want - placing it under the bottom step on a metal stairway means that no-one will be able to see it unless they get down on their hands and knees to do so.

    Nano caches are ideally suited for built up areas or urban-caching where you can find more places to site the magentic cache than in the countryside.

    Here are some ideas for you:

    * Under a park bench.
    * Under some steps.

* Under a bridge.
* Attach it to some railings.
* On a fence post.

Remember that just because it's magnetic doesn't mean you can't put it a hidey hole somewhere.

Make sure that you don't place it where workmen will find it. Trust me if a BT engineer comes to look into one of their boxes he will immediately spot anything out of place on it and you risk losing the cache. The cache should be placed out of the way.

Anti-forensic precautions

As with Postal or Courier sent messages, you might also need to take precautions against leaving characteristic DNA, fingerprint, fibre , particle etc. on the Container or the actual message itself.

Caches or Dead Drops outside, exposed to the weather, will probably involve metal or plastic etc. waterproofing, which usually retains fingerprints and DNA samples etc. quite well.

Anything sticky e.g. tape or adhesive used to weatherproof or attach the container to something, could also trap fibres, dust particles, hair, skin cells etc.

Signals about Caches or Dead Drops

See the section on Covert Channel Signals for Meetings or Dead Letter Drops for some ideas about Covert Channel Signals,

There may need to be different signals to signal that there is something at the Dead Drop to be picked up, that the Dead Drop is suspected of being under surveillance, and that an alternative Dead Drop should be used instead, or that an urgent Physical Meeting is needed..

In spy fiction and in real life espionage cases, such signals usually involve something inconspicuous, which the other person can notice without stopping and reading a note e.g. a window with curtains, a venetian blind or a light switched on or off, a chalk mark, or thumb tack on the pavement or on a bit of street furniture like a litter bin or telegraph pole etc.

The internet provides a lot of alternative methods of sending or receiving a Covert Channel signal.

Dead drop

From Wikipedia, the free encyclopedia

Jump to: navigation, search

This article includes a list of references, related reading or external links, but **its sources remain unclear because it lacks inline citations**. Please improve this article by introducing more precise citations. *(December 2011)*

Dead drop spike

A **dead drop** or **dead letter box** is a method of espionage tradecraft used to pass items between two individuals using a secret location and thus does not require them to meet directly. Using a dead drop permits a case officer and agent to exchange objects and information while maintaining operational security. The method stands in contrast to the **live drop**, so called because two persons meet to exchange items or information.

Contents

[hide]

[edit] Overview

Spies have been known to use dead drops, using various techniques to hide items (such as money, secrets or instructions) and to signal that the drop has been made.

The system involves using signals and locations which have been agreed upon in advance. These signals and locations must be common everyday things to which most people would not give a second glance. The signal may or may not be located close to the dead drop itself.

The location of the dead drop could be a loose brick in a wall, a library book, a hole in a tree, or under a boulder etc. It should be something common and from which the items can be 'picked up' without the operatives being seen by a member of the public or the security forces who may be watching.

The signaling devices can include a chalk mark on a wall, a piece of chewing-gum on a lamppost, a newspaper left on a park bench etc. Alternatively, the signal can be made from inside the agent's own home e.g. hanging a distinctively colored towel from a balcony, or placing a potted plant on a window sill where it is visible to anyone on the street.

Aldrich Ames left chalk marks on a mail box located at 37th and R Streets NW in Washington, D.C. to signal his Russian handlers that he had made a dead drop. The number of marks on the

box prompted some local residents to speculate, somewhat jokingly, that it was used by spies.[*citation needed*]

The dead drop is often used as a cut-out device. In this use the operatives who use the device to communicate or exchange materials or information do not know one another and should never see one another. While this type of device is useful in preventing the capture of an entire espionage network, it is not foolproof. If the lower level operative is compromised he or she may reveal the location and signal for the use of the dead drop. Then the counter espionage agents simply use the signal to indicate that the dead drop is ready for pickup. They then keep the spot under continuous surveillance until it is picked up. They can then capture the operative who picked up the material from the dead drop.

The **dead drop spike** is a concealment device similar to a microcache which has been used since the late 1960s to hide money, maps, documents, microfilm, and other items. The spike is waterproof and mildew-proof and can be shoved into the ground or placed in a shallow stream to be retrieved at a later time.

[edit] Modern dead drop techniques

On January 23, 2006, the Russian FSB accused Britain of using wireless dead drops concealed inside hollowed-out rocks to collect espionage information from agents in Russia. According to the Russian authorities, the agent delivering information would approach the rock and transmit data wirelessly into it from a hand-held device, and later his British handlers would pick up the stored data by similar means.[1]

[edit] See also

- Espionage
- Dead Drop (USB)

[edit] References

- "Russians accuse 4 Britons of spying".International Herald Tribune. January 24, 2006. News report on Russian discovery of British "wireless dead drop".
- "Old spying lives on in new ways". BBC. 23 January 2006.
- Madrid suspects tied to e-mail ruse. International Herald Tribune. April 28, 2006.
- Military secrets missing on Ministry of Defence computer files

1. **^** Nick Paton Walsh, The Guardian (23). "Moscow names British 'spies' in NGO row". http://www.guardian.co.uk/world/2006/jan/23/russia.politics. Retrieved 8 April 2012.

Geocaching

From Wikipedia, the free encyclopedia

Jump to: navigation, search

Geocaching	
 International Geocaching Logo	
Nickname(s)	Caching
First played	May 3, 2000
Clubs	Yes
Characteristics	
Contact	No
Team members	optional
Mixed gender	Yes
Categorization	Outdoor Sports
Equipment	GPS receiver or GPS-enabled mobile device,[1] writing utensil
Olympic	No

Geocaching is an outdoor sporting activity in which the participants use a Global Positioning System (GPS) receiver or mobile device[2] and other navigational techniques to hide and seek containers, called "geocaches" or "caches", anywhere in the world.

It is a derivation of the outdoor sporting activity of Geotrekking.

A typical cache is a small waterproof container containing a logbook where the geocacher enters the date they found it and signs it with their established code name. Larger containers such as plastic storage containers (Tupperware or similar) or ammunition boxes can also contain items for trading, usually toys or trinkets of little value. Geocaching is often described as a "game of high-tech hide and seek"[*by whom?*], sharing many aspects with benchmarking, trigpointing, orienteering, treasure-hunting, letterboxing, and waymarking.

Geocaches are currently placed in over 200 countries around the world and on all seven continents, including Antarctica,[3] and the International Space Station.[4] After more than 12 years of activity there are over 1.7 million active geocaches published on various websites. There are over 5 million geocachers worldwide.[5]

Contents

[hide]

[edit] History

Geocaching is similar to the 150-year-old game letterboxing, which uses clues and references to landmarks embedded in stories. Geocaching was conceived shortly after the removal of Selective Availability from GPS on May 2, 2000, because the improved accuracy[6] of the system allowed for a small container to be specifically placed and located. The first documented placement of a GPS-located cache took place on May 3, 2000, by Dave Ulmer of Beavercreek, Oregon.[7] The location was posted on the Usenet newsgroup[8][9] as

45°17.460'N 122°24.800'W45.291°N 122.4133°W. By May 6, 2000, it had been found twice and logged once (by Mike Teague of Vancouver, Washington). According to Dave Ulmer's message, the original stash was a black plastic bucket buried most of the way in the ground and contained software, videos, books, food, money, and a slingshot.[9]

The Oregon Public Broadcasting program Oregon Field Guide covered the topic of geocaching in a February 2010 episode, paying a visit to the original site.[10] A memorial plaque now sits at the actual site, the Original Stash Tribute Plaque (GCGV0P).

[edit] Origin of the name

The activity was originally referred to as *GPS stash hunt* or *gpsstashing*. This was changed after a discussion in the gpsstash discussion group at eGroups (now Yahoo!). On May 30, 2000, Matt Stum suggested that "stash" could have negative connotations, and suggested instead "geocaching."[11]

[edit] Geocaches

A Travel Bug from Hong Kong attached to a Common Stored Value Ticket.

For the traditional geocache, a geocacher will place a waterproof container containing a log book (with pen or pencil) and trade items then record the cache's coordinates. These coordinates, along with other details of the location, are posted on a listing site (see list of some sites below). Other geocachers obtain the coordinates from that listing site and seek out the cache using their GPS handheld receivers. The finding geocachers record their exploits in the logbook and online. Geocachers are free to take objects (except the logbook, pencil, or stamp) from the cache in exchange for leaving something of similar or higher value.

A Geocoin.

Typical cache "treasures" are not high in monetary value but may hold personal value to the finder. Aside from the logbook, common cache contents are unusual coins or currency, small toys, ornamental buttons, CDs, or books. Also common are objects that are moved from cache to cache called "hitchhikers", such as Travel Bugs or Geocoins, whose travels may be logged and followed online. Cachers who initially place a Travel Bug or Geocoins often assign specific goals for their trackable items. Examples of goals are to be placed in a certain cache a long distance from home, or to travel to a certain country, or to travel faster and farther than other hitchhikers in a race. Higher value items are occasionally included in geocaches as a reward for the First to Find (called "FTF"), or in locations which are harder to reach. Dangerous or illegal items, weapons, food and pornography are generally not allowed and are specifically against the rules of most geocache listing sites.

A Travel Bug

Geocache container sizes range from "nanos", which can be smaller than the tip of finger and only have enough room to store the log sheet, to 20 liter (5 gallon) buckets or even larger containers.[12] The most common cache containers in rural areas are lunch-box sized plastic storage containers or surplus military ammunition cans. Ammo cans are considered the gold standard of containers because they are very sturdy, waterproof, animal and fire resistant, relatively cheap, and have plenty of room for trade items. Smaller containers are more common in urban areas because they can be more easily hidden, the most common of these is the 35mm film canister.

A traditional geocache's hiding spot inside a stump.

If a geocache has been vandalized or stolen it is said to have been "muggled" or "plundered." The former term plays off the fact that those not familiar with geocaching are called muggles, a term borrowed from the *Harry Potter* series of books which was rising in popularity at the same time Geocaching got its start.[13]

[edit] Variations

Geocaches vary in size, difficulty, and location. Simple caches are often called "drive-bys," "park 'n grabs" (PNGs), or "cache and dash." Geocaches may also be complex, involving lengthy searches or significant travel. Examples include staged multi-caches;[14] underwater caches,[15][16] caches located 50 feet (15 m) up a tree,[17] caches found only after long offroad drives,[18] caches on high mountain peaks,[19] caches located in challenging environments (such as Antarctica [20] or north of the Arctic Circle[21]), and magnetic caches attached to metal structures and/or objects. Different geocaching websites list different variations per their own policies (e.g. Geocaching.com does not list new Webcam, Virtual, Locationless, or Moving geocaches). The traditional Geocaching gave birth to GeoCaching – one of active urban games of Encounter project. The game is quite similar to Geocaching but has time limitations and hints in it.

A small traditional geocache in the Czech Republic.

Variations of geocaches (as listed on geocaching.com and other popular listing sites) include:

- **Traditional/Basic:** Must include a log book of some sort. It may or may not include trade or traceable items. A traditional cache is distinguished from other cache variations in that the geocache is found at the coordinates given and involves only one stage.[22]

- **Multi-cache**: This variation consists of multiple discoveries of one or more intermediate points containing the coordinates for the next stage; the final stage contains the log book and trade items.[22]

    - **Offset**: This cache is similar to the multi-cache except that the initial coordinates are for a location containing information that encodes the final cache coordinates. An example would be to direct the finder to a plaque where the digits of a date on the plaque correspond to coordinates of the final cache.[22]

- **Mystery/puzzle**: This cache requires one to discover information or solve a puzzle to find the cache. Some mystery caches provide a false set of coordinates with a puzzle that must be solved to determine the final cache location. In other cases, the given location is accurate, but the name of the location or other features are themselves a puzzle leading to the final cache. Alternatively, additional information is necessary to complete the find, such as a padlock combination to access the cache.[22]

    - **Night Cache**: These multi-stage caches are designed to be found at night and generally involve following a series of reflectors with a flashlight to the final cache location.[*citation needed*]
    - **Challenge Cache**: These caches require that a geocacher complete a reasonably attainable geocaching-related task before being able to log the find. Examples include finding a number of caches that meet a category, completing a number of cache finds within a period of time, finding a cache for every calendar day, etc.[22]

- **Letterbox Hybrid**: A letterbox hybrid cache is a combination of a geocache and a letterbox in the same container. A letterbox has a rubber stamp and a logbook instead of tradable items. Letterboxers carry their own stamp with them, to stamp the letterbox's log book and inversely

stamp their personal log book with the letterbox stamp. The hybrid cache contains the important materials for this and may or may not include trade items. Whether the letterbox hybrid contains trade items is up to the owner.[22]

- **Locationless/Reverse**: This variation is similar to a scavenger hunt. A description is given for something to find, such as a one-room schoolhouse, and the finder locates an example of this object. The finder records the location using their GPS hand-held receiver and often takes a picture at the location showing the named object and his or her GPS receiver. Typically others are not allowed to log that same location as a find.[22]

- **Moving/Travelling**: Similar to a traditional geocache, this variation is found at a listed set of coordinates. The finder uses the log book, trades trinkets, and then hides the cache in a different location. By updating this new location on the listing, the finder essentially becomes the hider, and the next finder continues the cycle. The hitchhiker concept (see above) has superseded this cache type on geocaching.com.[*citation needed*]

A Geocacher finding a Virtual Cache at McMurdo Station, Antarctica

- **Virtual**: Caches of this nature are coordinates for a location that does not contain the traditional box, log book, or trade items. Instead, the location contains some other described object. Validation for finding a virtual cache generally requires you to email the cache hider with information such as a date or a name on a plaque, or to post a picture of yourself at the site with GPS receiver in hand.[22]

- **Earthcache**: A type of virtual-cache which is maintained by the Geological Society of America. The cacher usually has to perform a task which teaches him/her an educational lesson about the earth science of the cache area.[22]

- **Webcam**: Similar to a virtual cache; there is no container, log book, or trade items for this cache type. Instead, the coordinates are for a location with a public webcam. Instead of signing a log book, the finder is often required to capture their image from the webcam for verification of the find. Webcam geocaches are no longer part of Geocaching.com . Webcam caches are now part of another Groundspeak program known as Waymarking. These caches can be searched for on www.waymarking.com .[22]

- **Event Cache**: This is a gathering organized and attended by geocachers. Physical caches placed at events are often active only for the event date.[22]
    - **Cache-In Trash-Out (CITO) Events**: This variation on event caching is a coordinated activity of trash pickup and other maintenance to improve the environment.[22]
    - **Mega Event**: An event that is attended by over 500 people. Mega Events are typically annual events, usually attracting geocachers from all over the world.[22]
    - **GPS Adventures Maze Exhibit**: An exhibit at various museums and science centers in which participants in the maze learn about geocaching. These "events" have their own cache type on Geocaching.com and include many non-geocachers.[22]
- **Wherigo cache**: A Wherigo cache is similar to a multi-stage cache hunt that uses a Wherigo cartridge to guide the player. The player plays the cartridge and finds a physical cache sometime during cartridge play, usually at the end. Not all Wherigo cartridges incorporate geocaches into game play. Wherigo caches are unique to the geocaching.com website.[22]
- **BIT Cache**: Physical yet containerless caches, they are laminated cards with a URL and the password needed for logging. More information is available at www.BITcaching.com. They are listed exclusively on Opencaching.us.
- **Guest Book Cache**: Physical guest books often found in museums, tourist information centers, etc. They are listed exclusively at Opencaching.us.
- **USB Cache**: Paperless caches stored inside USB drives and embedded (with permission) into walls or other structures. The cache is retrieved by connecting a device that has a USB port and that is able to read standard text files. Also known as Dead Drop caches.

[edit] Obtaining data

GPX files containing information such as a cache description and information about recent visitors to the cache are available from various listing sites. Geocachers may upload geocache data (also known as waypoints) from various websites in various formats, most commonly in file-type GPX, which uses XML.[23] Some websites allow geocachers to search (build queries) for multiple caches within a geographic area based on criteria such as Zip Code or coordinates, downloading the results as an email attachment on a schedule. In the recent years, Android and iPhone users have been able to download apps such as GeoBeagle[24] that allow them to use their 3G/Gps enabled devices to actively search for and download new caches.

[edit] Converting and filtering data

A variety of geocaching applications are available for geocache data management, file-type translation, and personalization. Geocaching software can assign special icons or search (filter) for caches based on certain criteria (e.g. distance from an assigned point, difficulty, date last found).

Paperless geocaching means hunting a geocache without a physical printout of the cache description. Traditionally, this means that the seeker has an electronic means of viewing the cache information in the field, such as pre-downloading the information to a PDA or other electronic device. Various applications are able to directly upload and read GPX files without further conversion. Newer GPS devices released by Garmin, DeLorme and Magellan have the ability to read GPX files directly, thus eliminating the need for a PDA.[25] Other methods include viewing real-time information on a portable computer with internet access or with a web-enabled smart phone. The latest advancement of this practice involves installing dedicated applications on a smart phone with a built-in GPS receiver. Seekers can search for and download caches in their immediate vicinity directly to the application and use the on-board GPS receiver to find the cache.

A more controversial version of paperless caching involves mass-downloading only the coordinates and cache names (or waypoint IDs) for hundreds of caches into older receivers. This is a common practice of some cachers and has been used successfully for years. In many cases, however, the cache description and hint are never read by the seeker before hunting the cache. This means they are unaware of potential restrictions such as limited hunt times, park open/close times, off-limit areas, and suggested parking locations.

[edit] Mobile Devices

The website geocaching.com[26] now sells mobile applications which allow users to view caches through a variety of different devices. Currently, the Android, iPhone, webOS, and Windows Phone 7 mobile platforms have applications in their respective stores. The app also allows for a trial version with limited functionality. Additionally "c:geo - opensource"[27] is a free opensource full function application for Android phones that is very popular.

Geocaching enthusiasts have also made their own hand-held GPS devices using a Lego Mindstorms NXT GPS sensor.[28][29]

[edit] Souvenirs

In mid-2010, Groundspeak added the souvenir feature to the website. By finding certain caches or finding caches on a certain date, a geocacher earns a special icon which is posted on that cacher's profile page.

[edit] Geodashing

Geodashing is an outdoor sport in which teams of players use GPS receivers to find and visit randomly-selected "dashpoints" (also called "waypoints") around the world and report what they find. The objective is to visit as many dashpoints as possible.[30][31]

Unlike geocaching, nothing is to be left at the dashpoints; the sole objective is to visit them within the time limit.[32][33]

The first game organized by gpsgames.org[34] ran for two months (June and July 2001); each subsequent game has run for one month. Players are often encouraged to take pictures at the dashpoints and upload them to the site.

[edit] Terminology

There are various acronyms and words commonly used when discussing geocaching.

General:

- **Cache** – A box or container that contains, at the very least, a logbook.
- **Geoswag** – The items that can be found in some larger caches.
- **Georing** – A term first coined by the South GA Geocachers group in 2011. It's the term used to refer to a notification tone made by a smartphone when a new cache is published.
- **Muggle** – A non-geocacher.
- **Muggled** - Being caught by a non-geocacher while retrieving/replacing a cache; also, a muggled cache has been removed or vandalized by a non-geocacher, usually out of misunderstanding or lack of knowledge.
- **Smiley** – A cache find. Refers to the "smiley-face" icon attached to "Found It" logs on some listing sites.
- **BYOP** – (Bring Your Own Pen/Pencil) The cache in question lacks a writing device for the logbook.
- **CITO** – (Cache In Trash Out) and refers to picking up trash on the hunt.
- **CO** – (Cache Owner) The person who is responsible for maintaining a cache, usually the person who hid it.
- **DNF** – (Did Not Find) Did not find the cache container being searched for.
- **FIGS** - Found in good shape.
- **FTF** – (First To Find) The first person to find a cache container; less commonly one may see STF (second to find, or TTF, third to find).
- **FTL** – (First To Log) The first person to log the find of a cache container online.
- **GPS** – Short for Global Positioning System, also occasionally refers to the receiver itself.
- **GPSr** – Short for GPS receiver.
- **PAF** - Phone-A-Friend.
- **SGC** - (Senior Geocacher) An experienced participant of the pursuit.

Logging a hunt:

- **TFTC** – (Thanks For The Cache) This is often used at the end of logs to thank the cache owner.
- **TFTH** – (Thanks For The Hunt or Hide or Hike) It shares the same purpose as TFTC, but can also be used when the cache was not found.
- **TN** – (Took Nothing) no trade or traveling item was removed from the cache.
- **LN** – (Left Nothing) no trade or traveling item was added to the cache.
- **XN** – (eXchanged Nothing) combines the previous two acronyms; nothing was removed or added.
- **SL** – (Signed Log) used when the participant visited the cache and signed its logbook.
- **TSIA** – (The Streak is Alive) used when the participant has an active streak of continuous days finding a cache.

Note: the various acronyms in this section are often combined in various ways, such as "TNLNSL, TFTC!"

Location description or hint:

- **GRC –** (GuardRail Cache) used in the description on where a cache may be hidden.
- **GZ –** (Ground Zero or Geo-zone) refers to the general area in which a cache is hidden. For Example:- The cache is hidden at N50 35.195 W003 27.961
- **ICT –** (Ivy Covered Tree) used in the description on where a cache may be hidden.
- **LPC –** (Light/Lamp Post Cache) used in the description on where a cache may be hidden.
- **MKH –** (Magnetic Key Holder) used in the description on the type of container used for the cache.
- **P&G** - (Park and Grab) used to refer to a cache that is fairly close to the nearest parking spot, does not require hiking more than a tenth of a mile
- **PLC –** (Parking Lot Cache) used in the description on where a cache may be hidden.
- **POR –** (Pile Of Rocks) used in the description on where a cache may be hidden.
- **POS –** (Pile Of Sticks or Stones) used in the description on where a cache may be hidden.
- **SL** - (Skirt Lifter) refers to the metal or plastic skirt at the base of a lightpole, and used in reference to LPC caches (see LPC).
- **SOOP** - (Something Out of Place) used to refer to a natural or other object that seems out of place, indicating a geocache is hidden in that spot
- **TOTT** - (Tool of the Trade) can refer to any out of the ordinary tool needed/used to retrieve a cache. Most often used tongue-in-cheek to refer to the use of a ladder to get to an out-of-reach cache.
- **UFO –** (Unnatural Formation of Objects) a pile of material that obviously did not form naturally and is a likely cache hiding spot.
- **UPS –** (Unnatural Pile of Sticks) a piles of sticks that did not form naturally and where a cache may be hidden.[35]

[edit] 10/10/10

On 10 October 2010 geocachers around the world held events and went caching to commemorate 10 years of geocaching. In the process they set a record for the most geocachers to find a cache in a day, with 78,313 accounts logging a cache.[36]

[edit] Leap Day

For many geoacachers, Leap Day offers a unique opportunity to find a geocache. On 29 February 2012, a new record for the most geocachers to find a cache in a single day was set when 83,516 accounts logged a cache, breaking the record that had previously been set on 10 October 2010.[37] This was more than double the 36,696 accounts that logged a cache on Leap Day 2008.[38]

[edit] Ethics

Individual geocaching websites have developed their own guidelines for acceptable geocache publications. Though not universally required, the *Geocacher's Creed*[39] provides ethical search guidelines. Government agencies and others responsible for public use of land often publish

guidelines for geocaching.[40][41] Generally accepted rules are to not endanger others, to minimize the impact on nature, to respect private property, and to avoid public alarm.

[edit] Controversy and issues

Cachers have been approached by police and questioned when they were seen as acting suspiciously.[42][43] Other times, investigation of a cache location after suspicious activity was reported has resulted in police and bomb squad discovery of the geocache. Schools have been occasionally evacuated when a cache has been seen by teachers or police, as in the case of Fairview High School in 2009.[44][45][46] A number of caches have been destroyed by bomb squads.[47][48][49]

The placement of geocaches has occasional critics among some government personnel and the public at large who consider it littering. Some geocachers act to mitigate this perception by picking up litter while they search for geocaches, a practice referred to in the community as CITO (Cache-In-Trash-Out). Events and caches are often organized revolving around this practice, with many areas seeing significant cleanup that would otherwise not take place, or would instead require federal, state or local funds to accomplish. Geocachers are also encouraged to clean up after themselves by retrieving old containers once a cache has been removed from play.

Geocaching is not illegal in the United States and is usually positively received when explained to law enforcement officials. However, certain types of placements can be problematic. Although generally disallowed, hiders could place caches on private property without adequate permission (intentionally or otherwise), which encourages cache finders to trespass. Caches might also be hidden in places where the act of searching can make a finder look suspicious (e.g. near schools, children's playgrounds, banks, courthouses, or in residential neighborhoods), or where the container placement could be mistaken for a drug stash or a bomb (especially in urban settings, under bridges, near banks, courthouses, or embassies). As well as concerns about littering and bomb threats, some geocachers hide their caches in inappropriate locations, that may encourage risky behaviour, especially amongst children. Examples include electrical boxes and light pole covers.[50] Hides in these areas are discouraged,[45] and cache listing websites enforce guidelines that disallow certain types of placements. However, as cache reviewers typically cannot see exactly where and how every particular cache is hidden, problematic hides can slip through. Ultimately it is also up to cache finders to use discretion when attempting to search for a cache, and report any problems.

The South Carolina House of Representatives passed Bill 3777[51] in 2005, stating, "It is unlawful for a person to engage in the activity of geocaching or letterboxing in a cemetery or in an historic or archeological site or property publicly identified by an historical marker without the express written consent of the owner or entity which oversees that cemetery site or property." The bill was referred to committee on first reading in the Senate and has been there ever since.[52]

[edit] Websites and Data Ownership

Numerous websites list geocaches around the world. In the United States, where most geocaching services are hosted, only a cache's coordinates are in public domain. Other cache information, including the description, is protected by copyright law. Geocaching websites vary in active protection of cache data.

[edit] First page

The first website to list geocaches was announced by Mike Teague on May 8, 2000. On September 2, 2000, Jeremy Irish emailed the gpsstash mailing list that he had registered the domain name geocaching.com and had set up his own Web site. He copied the caches from Mike Teague's database into his own. On September 7, Mike Teague announced that Jeremy Irish was taking over cache listings.

[edit] Geocaching.com

GPS receivers from Trimble, Garmin. and Leica.

Container displaying the official Geocaching.com logo.

The largest site is Geocaching.com, owned by Groundspeak Inc., which began operating on September 2, 2000. With a worldwide membership, the website lists more than 1.8 million caches in over 200 countries around the world as of June, 2012. Each cache is reviewed by regional cache reviewers before publication. Free basic membership allows users to see coordinates for most caches in its database; premium membership includes a fee for additional features, including advanced search tools and caches designed for premium members.

The website no longer lists new caches without a physical container, including virtual and webcam caches; however, older caches of these types have been grandfathered in (except for locationless/reverse, which are completely archived). Earthcaches are the exception to the no-

container rule; they are caches in which players must answer geological questions to complete the cache. Groundspeak created a waymarking website to handle all other non-physical caches.

The website also supports the discovery of benchmarks in the USA.[53] There are currently no benchmarks outside the USA in their database. The website provides the best known longitude and latitude (sometimes only accurate to within six or more seconds) of the object along with a description. Hunters use the clues to try to find the benchmark; the benchmark can be logged as Found, Not Found, Note, or Destroyed. The "Destroyed" log should only be used if there is evidence that the mark has been permanently destroyed.

Groundspeak allows extraterrestrial caches, e.g. the Moon or Mars, although the website only presently provides earthbound coordinates. Thus the cache that exists on the International Space Station, GC1BE91,[54] uses the Russian launch area as its position.

Geocaching.com has been criticized for its uncooperative stance towards mobile application developers,[55] and for continuously delaying the release of a promised open API.[56] Some progress has been made recently, with the site now promoting mobile applications branded as Geocaching Live Enabled, and listing over a dozen applications (both mobile and browser/desktop based) that are using their newly released public API.[57] The controversy continues, as developers have criticised Geocaching Live for being incompatible with open-source development,[58] among other things.

[edit] NaviCache

Navicache.com started as a regional listing service around February 2001, but quickly gained popularity among those looking for a less restrictive alternative to what was currently available. While many of the websites listings have been posted to other sites, they also offer many unique listings. The website lists nearly any type of geocache (within reason) and does not charge to access any of the caches listed in their database. While all submissions are reviewed and approved, Navicache is more liberal in approving caches believing that the pastime belongs to participants rather than a governing agency.

[edit] Opencaching Network

The Opencaching Network provides independent, non-commercial listing sites based in the cacher's country or region. The Opencaching Network lists the most types of caches, including traditional, virtual, moving, multi, quiz, webcam, BIT, guest book, USB, event and MP3. The Opencaching Network is less restrictive than many sites, and does not charge for the use of the sites. All listings are reviewed by the network operators before being published and although cross-listing is permitted, it is discouraged. Some listings are listed on other sites, but there are many that are unique to the Opencaching Network. Features include the ability to organize your favorite caches, build custom searches, be instantly notified of new caches in your area, seek and create caches of all types, export GPX queries, statpics, etc. Each Opencaching Node provides the same API for free (called "OKAPI"[59]) for developers who want to create third-party application with Opencaching Network's content.

[edit] TerraCaching

Terracaching seeks to provide high-quality caches made so by the difficulty of the hide or from the quality of the location. Membership is managed through a sponsorship system, and each cache is under continual peer review from other members. Terracaching.com embraces virtual caches alongside traditional/multi-stage caches and includes many locationless caches among the thousands of caches in its database. It is increasingly attracting members who like the point system. In Europe TerraCaching is supported by Terracaching.eu. This site is translated in different European languages, has an extended FAQ and extra supporting tools for TerraCaching.

Terracaching does not allow caches that are listed on other sites, so called double-listing.

[edit] GPSgames

GPSgames is a more open geocaching website that allows the geocaching community more flexibility in the types of geocaches placed. The traditional geocaches are more common, but, virtual, locationless, and traveler geocaches are still allowed. Other GPS games are also available. Geodashing, Shutterspot, GeoVexilla, MinuteWar, GeoPoker, and GeoGolf are among the other GPS games available.

[edit] AdventureGeoGolf.com GPS Game

First of its kind in the World Adventure GeoGolf game is a GPS geocaching game played by geocachers who will go out and find 18 traditional cache hides on a virtual golf course in order to log their find on Geocaching.com The first GeoGolf game course is being built in Dubai, UAE.

[edit] Opencaching.com

Not to be mistaken for opencaching.us, opencaching.com aims to be as free and open as possible with no paid content. Caches are approved by a community process and coordinates are available without an account. Traditional, puzzle, virtual, and multi caches are supported. All caches published on opencaching.com are available under an Open Source license. The site was created by Garmin, but owning a Garmin device is not required for the full use of the site, as there are several Android and iPhone apps that lets users access the site while on the trail.

Opencaching.com also provides a free API[60] for developers that want to utilize the site's content.

Opencaching.com does allow caches that are listed on other sites, so called double-listing.

[edit] Other sites

In many countries there are regional geocaching sites, but these mostly only compile lists of caches in the area from the three main sites. Many of them also accept unique listings of caches for their site, but these listings tend to be less popular than the international sites, although occasionally the regional sites may have more caches than the international sites. There are some

exceptions though, e.g. in the former Soviet Union the site Geocaching.su remains popular because it accepts listings in the Cyrillic script. Additional international sites include Geocaching.de, a German website, and Geocaching Australia, which accepts listings of cache types depreciated by geocaching.com as well as traditional geocaches.

Covert Channel Signals for Meetings or Dead Letter Drops

Covert Channel Signals for Dead Drops or Physical Meetings

Unless you have established a regular schedule for checking to see if anything has been left in a Dead Letter Drop, its use will usually require some sort of Covert Channel Signal.

In spy fiction and in real life espionage cases, such signals usually involve something inconspicuous, which the other person can notice without stopping and reading a note e.g. a window with curtains, a venetian blind or a light switched on or off, a chalk mark, or thumb tack on the pavement or on a bit of street furniture like a litter bin or telegraph pole, leaving a car parked in a certain parking space, or literally flying a flag. etc.

There may need to be different signals to communicate that there is something at the Dead Drop to be picked up, that the Dead Drop is suspected of being under surveillance, that an alternative Dead Drop should be used instead, or that an urgent Physical Meeting is needed..

Obviously all sorts of misunderstandings and errors can happen, especially if this users of the Dead Drop ave not practiced the technique much, or at all.

Internet Covert Channel Signals

Covert Chanel Signals can be as simple as changing one bit in a computer file from a Zero to a One (or vice versa), and pre-arranging,in secret, what this means, and when and where such a signal is valid, so there are lots of possibilities offered by the internet or telecommunications systems.

The Geo-cachers, of course, can use a website with email and rss syndication feed or even SMS text message notification, to announce to the world that a new cache has been created, ir filled. The internet provides lots of possible Covert Channel Signal,e.g. the fact that a message mentioning a pre-arranged code word or phrase is posted to a public discussion forum or to an email account , perhaps disguised as spam / junk mail advertising etc.

The internet and the world wide web offers a plethora of free email accounts, free disk space for file sharing, free web blogs etc. which can be used relatively anonymously, by more than one person (if the username and password details are shared, to provide such a Dead Drop facility for sending messages covertly. The legalities of snooping on file transfers which are not specifically "electronic communications" like email, is a bit unclear under UK law, but if you are under suspicion,the chances are that it will happen, even if it cannot be used directly as evidence in court. N.B. in the UK, the use of electronic intercept cannot be used as evidence in Court (it can obviously be used for investigations), but the use of Communications traffic Data and anayses can be used in Court.

Multi-user blogging or forum software can legitimately provide an excuse for different people to log into the system, at different times, from different IP addresses, in order to browse and "edit" articles "for publication". Provided that some blog articles or forum messages are actually published, an act which in itself might be a Covert Channel Signal, then such activity may not raise any suspicions.

N.B. If editing an external blog,or uploading file to say,, a photo file sharing service, is prohibited or unusual, in your corporate of government office, then it might draw attention to you as a potential whistleblower leak suspect.

These internet techniques have probably superceded the use of small adverts in the Personal Columns of printed newspapers and magazines, although offering something for sale via , say, the Loot Classified Ads website, or via phone, might still be a useful technique sometimes.

Deliberately Missed Phone Calls

One old Covert Channel technique , which is under surveillance automatically by the telrcomms companies (fto see if there is a problem with the infrastructure in a particular area, or to investigate possible loss of revenue) and therefore also by state authorities is the old technique of letting a telephone ring a certain number of times, before ringing off.

This dates back to the earliest fays of the landline telephone, and can be used to convey standard, pre-arranged messages such as "I am catching the train home in the next few minutes, start cooking dinner" etc., It has the advantage of not costing any money, as phone calls are not usually charged until the receiving party picks up and answers the call,. This technique is popular in Africa, where it sometimes called "beeping" of "flashing".Many poor people make use of it, exploiting the Caller ID feature of even missed phone calls, to identify which phone has just "beeped" you for free, to such an extent that a system of etiquette has evolved e.g. it is not considered to be ethical to "beep" someone who you know has very little or no mobile phone credit - the "beep" may be free, but not if it signals "phone me back as soon as possible".

In the UK, people are usually rich enough not to be so worried about this, but from a whistleblower / journalist / activist contact anonymity point of view, it might be better not reply to such a Covert Channel signal, except via a different Covert Channel method, ideally, not immediately upon receipt of the first Cover Channel tipoff message.

However, the European Union Data Retention Directive, and the previous UK Government Voluntary Code of Practice, (under the Anti-terrorism, Crime and Security Act 2001), **specifically mentions retaining "failed call attempts"**, so this is all likely to be **automatically logged** for at least a year.

Since you can never be sure if or, or how thoroughly, an **Answerphone or Voice Mailbox** message is ever **erased**, then it might be best to **avoid using these as Dead Drops** for messages, unless you can disguise your voice and have a pre-arranged series of code phrases, which sound innocuous.

Postal mail and Courier services

"Inform the queen!" said Athos; "and how? Have we relations with the court? Could we send anyone to Paris without its being known in the camp? From here to Paris it is a hundred and forty leagues; before our letter was at Angers we should be in a dungeon."

"As to remitting a letter with safety to her Majesty," said Aramis, coloring, "I will take that upon myself. I know a clever person at Tours--"

Aramis stopped on seeing Athos smile.

"Well, do you not adopt this means, Athos?" said d'Artagnan.

"I do not reject it altogether," said Athos; "but I wish to remind Aramis that he cannot quit the camp, and that nobody but one of ourselves is trustworthy; that two hours after the messenger has set out, all the Capuchins, all the police, all the black caps of the cardinal, will know your letter by heart, and you and your clever person will be arrested."

Chapter 47, The Council of the Musketeers, *The Three Musketeers*, by Alexandre Dumas, 1844 - text available online via Project Gutenberg

Mail Interception

Some national Post Office services have literally hundreds of years of experience of intercepting letters on behalf of the state or the police etc. For targeted investigations, they have the skills and technology to copy a letter in a sealed envelope, or to make a good copy of a sealed envelope which they have had to destroy when opening it..

It is impractical to intercept lots of postal mail, a much more difficult task than intercepting emails or phone calls, so these powers are reserved for serious cases, such as drug smugglers, terrorists and, unfortunately, Government whistleblowers.

In the United Kingdom, this Postal Communications Interception is covered by the "Regulation of Investigatory Powers Act 2000 section 19 Offence for unauthorised disclosures , with a penalty of up to 2 years in prison for "tipping off" anyone about the existence of or details of an interception warrant (which needs to be rubber stamped by the Home Secretary or a Home Office official), just like phone or email content tapping.

In the United Kingdom, Postal Communications Providers are required, by law, to:

Statutory Instrument 2002 No. 1931

The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002

[...]

Part I: Interception Capability for Public Postal Services

1. To ensure the interception and temporary retention of postal items destined for addresses in the United Kingdom for provision to the person on whose application the interception warrant was issued.

2. To provide for the interception and retention of postal items sent by identified persons where the carrier keeps records of who sent which item in the course of their normal business.

3. To maintain a system of opening, copying and resealing of any postal item carried for less than £1.

4. To comply with the obligations set out in paragraphs 1 to 3 above in such a manner that the chance of the interception subject or other unauthorised persons becoming aware of any interception is minimised.

Postal Mail anti-forensics precautions

- Licking a Postage Stamp is likely to leave both your fingerprints on it, and to preserver a sample of your DNA from your saliva.

- Sealing a letter envelope or parcel, or affixing a postage stamp using sticky adhesive tape or glue etc. will also tend to trap possibly identifiable fibres, dust particles, hairs, skin cells and fingerprints (which may contain sufficient DNA for analysis) , or even a characteristic scent which could be used by tracker dogs.
- A single sheet letter, in an envelope with the seal along the long edge, is relatively easy to extract, examine / copy and then re-insert, simply by rolling it up with tweezers etc, and removing it through the gap in the adhesive designed to allow for the insertion of a letter opener. Obviously, with multiple sheets of paper, stapled together, in envelopes with the sealed flap along the short side, it is often impossible to do this, and the usual steaming and re-sealing techniques (or if, all else fails, a completely new envelope) would then be used
- As pointed out by irdial. Self adhesive "peel off" postage stamps are increasingly common these days and there are also now "over the counter" laser printed postage stamps and also ones which can be downloaded and printed from a web page. Such on demand printed postage stamps, and even some franking machine stamps leave a potentially traceable serial number audit trail.
- What is true for postage stamps, also applies to sealing the flap of an envelope, to Air Mail stickers, Registered Post stickers, various address labels, or any use of self adhesive tape to wrap up a parcel or packet or letter.
- irdial also suggest:

> Do not use envelopes from a sealed pack. There are many places where you can buy packs of envelopes that are not sealed. In fact, these are often displayed adjacent to the Post Office queue. Why should you do this? If you use one of these loose envelopes, you can be sure that the sneezes, browsing touches, hairs and and breath traces of tens of thousands of people are going to be on them. These envelopes will be hopelessly contaminated, and that is good for you.

- Sometimes the source of your envelopes may actually be easy to trace, especially if like this malicious hoaxer Naser Ahmed, who was convicted under the Malicious Communications Act 1988, you send several postal letter threats and hoaxes "using a specific kind of envelope that was only available from one Post Office department."
- It is therefore a good idea to use gloves (and a facemask, and a hair net etc. - just as if you were handling uncontaminated food or biological laboratory samples) when touching a letter or envelope, especially as the latent fingerprint techniques have been improved recently e.g. through the use of di-sulpher di-nitride S2N2 polymer, which can "develop even very faint traces of fingerprints.. This appears to a an improvement on previous techniques for developing latent fingerprints on difficult surfaces e.g. absorbent paper, over say, "superglue" or iodine vapour fumes.
- S2N2 polymer is so sensitive, that it can pick up latent images of inkjet printed text from a letter or document which has been transferred to the **inside of an envelope** This sort of ink transfer, which is not visible to the naked eye, is something to watch out for if you decide to re-use otherwise untraceable envelopes, or if you print you whistleblowing document to a network printer - you may transfer traceable information to or from your whistleblower document, if it is printed in the middle of a stack of other print jobs at the same time.

Posting your mail

Mailing a whistleblower leak document requires careful choice of a post box. An out of the way rural post box, where strangers stand out as being potentially suspicious, may actually be less anonymous than a very busy urban one, in spite of the extra chances of CCTV surveillance footage..

Some large organisations have very lax internal mail systems (e.g. HMRC, which managed to lose the CDs with copies of the entire national Child Benefit database on them) , which could allow a whistleblower to simply mail an external mail envelope to their journalistic or other contacts from

work, with a high degree of anonymity, especially one already franked or stamped, which is then handled by lots of people before it is sent out via the postal mail service or private courier systems.

Receiving whistleblower postal mail

Receiving whistleblower documents by mail at your normal business or home address is , of course, not advisable, if you are trying to protect your sources.

Commercial Postal Box rental, either from a private company or for an extra fee from the state postal service, has its place, but there is always a financial paper trail to the person who rents the box, and often CCTV video footage of anyone picking up mail from such boxes.

Wikileaks Postal Submissions

Wikileaks.org offers a supposedly secure Postal Whistleblowing service, for whistleblower leaks to them, but they do not seem to recommend many anti-forensics precautions. except regarding the serial numbers embedded into batches of CDROMs, and the unique Recorder IDs which most CD or DVD burners embed in each copy which they produce..

WikiLeakS.org - no longer functioning for whistleblowers

WikiLeakS.org

As of 2010 the WikiLeakS.org project **no longer bothers to accept new submissions** from whistleblowers.

They seem to have censored themselves and **no longer publish** the whistleblower documents which they had accepted and published on their wiki.

They seem to be concentrating purely on hyping and presenting the treasure trove of journalistic scoops, which have seemingly emanated from a single source, a low level US Army intelligence analyst, Bradley Manning, who seems to have exploited his privileged access to SIPRENET to access a vast array of Afghan war, Iraq war and US diplomatic cables.

He then betrayed his own identity and links to wikileaks.org, through IRC sessions with the publicity seeking convicted computer hacker Adrian Lamo, who, unsurprisingly, decided to inform the US authorities.

The reaction of the US Government has been to try too "shoot the messenger" instead of sorting out their own computer security and personnel management systems.

If such a naive and unprofessional whistleblower could leak so much information, then foreign intelligence agencies and serious organised criminals must have access to lots of of US military intelligence secrets.

Perhaps there will be another WIkileaks.org type website, which has learned from their success and mistakes, but until then, **steer well clear of Wikileaks.org**, if you are a whistleblower - you will not get published and you will be trying to contact people who are already notorious and under intense surveillance and pressure.

N.B. as of 12th June 2010, WikiLeakS.org no longer have any of their secure online whistleblower leak document submission methods in operation: - no PGP, no Tor Hidden Service, no SSL/TLS Digital Certificate encrypted https://secure.wikileaks.org web URL.

They have also switched off their Discussion pages, so they are no longer even a "wiki" website.

So all the stuff below is academic - **WikiLeakS.org is no longer functioning,** except as a one way Twitter propaganda campaign.

There has been quite a bit of mainstream media and blogosphere coverage of the WikiLeakS.org project which makes bold claims:

Wikileaks is an uncensorable version of Wikipedia for untraceable mass document leaking and analysis. It combines the protection and anonymity of cutting-edge cryptographic technologies with the transparency and simplicity of a wiki interface.

Wikileaks looks like Wikipedia. Anybody can post comments to it. No technical knowledge is required. Whistleblowers can post documents anonymously and untraceably. Users can publicly discuss documents and analyze their credibility and veracity. Users can discuss the latest material, read and write explanatory articles on leaks along with background material and context. The political relevance of documents and their veracity can be revealed by a cast of thousands.

Wikileaks incorporates advanced cryptographic technologies to ensure anonymity and untraceability. Those who provide leaked information may face severe risks, whether of political repercussions, legal sanctions or physical violence. Accordingly, sophisticated cryptographic and postal techniques are used to minimize the risks that anonymous sources face.

For the technically minded, Wikileaks integrates technologies including modified versions of MediaWiki, OpenSSL, FreeNet, Tor, PGP and software of our own design.

Wikileaks information is distributed across many jurisdictions, organizations and individuals. Once a document is leaked it is essentially impossible to censor.

It has been used to leak some copies of documents and analyses to do with Guantnamo Bay or the US Military in Iraq or a suppressed report about corrupt politicians in Kenya etc.

They have been the source of a couple of front page newspaper stories, i say,,, The Guardian or the New York Times.

WikiiLeakS.org have, so far, fought off an attempt by a Swiss Bank and their Hollywood media reputation lawyers, to shut them down through the Federal Court in California, by legally restraining their main brand name Internet Domain Name. This was something which foundered on the US First Amendment to the constitution freedom of speech, freedom of the press , almost no prior restraint of publication laws. Their servers are currently in Sweden

WikiLeaKS.org has been used to leak a couple iof UK specific documents, one from the Home Office Identity and Passport Service. about the wretched National Identity Register / ID cards scheme and one which was subject to a UK High Court injunction against the mainstream press and media, regarding the now obsolete investment prospectus for the failed and now nationalised bank Northern Rock plc.

So has this project made traditional whistleblowing and leaking and getting stories from confidential Government or Corporate sources obsolete ? Not at all, there are plenty of unanswered questions about WikiLeakS.org

See the WikiLeak.org blog (no "S") for discussion of the technical, legal and ethical problems which the project raises.

At the moment, WikiLeakS.org may be of some use to a UK Government whistleblower who only risks his or her job, and not a stiff prison sentence, provided that they take some of the precautions in this Hints and Tips guide.

WikiLeakS.org is not yet trustworthy or demonstrably secure enough, to risk your life or that of your family.

LeakDirectory.org wiki

Following the spectacular media hype and journalistic scoops which the controversial WikiLeaks.org project has helped to create, there is still a demand for such Anonymous, Secure and Effective whistleblower leak submission and publication services.

WikiLeakS.org, whilst it is still doling out the vast cache of US Government diplomatic cables it has acquired, is no longer of any use to "ordinary" whistleblowers - they no longer have any functioning leak submission or publication system at all.

The WikiLeaks.org cult has inspired several other, more limited projects, which will hopefully learn from the successes and mistakes made by Julian Assange and his former associate Daniel Domscheit-Berg etc.

Links to many of these new independent whistleblower leak projects, to mainstream media whistleblower web sites and also to "official" government or public body anti-corruption or crime or terrorism or national security reporting websites, are available at the

Leak Directory wiki

Feel free to contribute to the risk and benefits analyses, of the good and bad points of these projects by editing the public wiki (which can be done reasonably anonymously).

Hopefully Leak Directory should be of use to careful potential Whistleblowers and to anyone setting up or running such a web site

Tor - The Onion Router cloud of proxy servers

Tor - The Onion Router cloud of proxy servers

UPDATED 05 May 2012

1. You may wish to make use of the Tor onion routing network, which can help to obscure your traceable IP address, when you are setting up or using a web email account e.g. Hushmail or Hotmail etc. It can also be useful if your whistleblowing activities are only low level ones, which might be appropriate as an anonymous comment published on a web blog.
2. The Vidalia bundle package makes it quite easy to install Tor and configure Tor via a GUI front end.
3. The bundled Privoxy or Polipo socks proxy helps to hide your DNS requests and the TorButton Firefox web browser add-in, helps to protect your anonymity from sneaky javascript, cookies and other attempt by a website to track repeated visitors.
4. From our web log statistics, it seems that some people are getting to this blog article by searching for the Tor download page, from countries where this may be blocked or censored. The list of official mirror sites is at:https://www.torproject.org/getinvolved/mirrors.html.en
5. Here is a mirror copy of the Tor Browser Bundle which is designed to work standalone, e.g. from a USB flash memory device, which comes with a privacy configured version of the Firefox web browser. Here is our mirror copy of the Tor Browser Bundle version 2.3.35-11 (about 21Mb)

   N.B. using the Tor Browser Bundle is now recommended, because of the difficulties that even the latest versions of TorButton have in keeping your session anonymous in the latest versions of the Firefox web browser, especially if you have lots of other plugins and extensions installed.

6. Remember to read and understand the warnings about the ways in which you can still betray your real IP address, even if you are using Tor.
7. If you have access to Hushmail or Google gmail or Yahoo mail or FastMail.FM (or any other email system which uses DKIM) then you can get a copy of the latest Tor software via an email to gettor@torproject.org

   See GetTor e-mail autoresponder
   or send an email with "help" in the body of the email to get instructions. Just put one or more of these request names in the body of the email (you can leave the subject line blank).

   panther-bundle
   source-bundle
   windows-bundle
   tiger-bundle
   tor-browser-bundle
   tor-im-browser-bundle

   The requested software will be sent back to you automatically via email, as an attached compressed .zip file archive.

8. Remember to verify the digital signatures of your Tor software in case it been accidentally corrupted in transit or has been maliciously substituted with a rogue copy.
9. If you are moderately technically adept, and have at least ADSL internet connectivity, you might wish to consider donating some of the bandwidth by running Tor as a server, either just to help mix up the traffic within the Tor "cloud" or also to offer your Tor server as an Exit Node (with the appropriate exit policy and bandwidth restrictions). By doing so, you will be helping potential whistleblowers and political dissidents living under repressive regimes. This is a moral choice, which, in our view, far outweighs the possible use of this system by criminals and terrorists.
10. In order to make censorship a little more difficult, a copy of this Spy Blog http://ht4w.co.uk Hints and Tips for Whistleblowers guide, is also being published as a Tor Hidden Service.

    http://46g2asmp7ouz2udv.onion/ (not guaranteed to be available available 24/7)

    You will need to have installed the Tor software and established a working Tor connection, and then you will be able access this copy via end to end encryption and a high degree of anonymity through the Tor cloud:

    Several of the post-WikiLeaks whistleblower websites already use, or plan to use of Tor Hidden Services e.g. BalkanLeaks.eu or the still not yet live OpenLeaks.org or GlobaLeaks.org

    See the LeakDirectory.org wiki for a listing these post-WikiLeaks websites and official government tipoff websites etc., together with anonymity and security analyses of some of the,

11. The former Labour Government's authoritarian legal powers have still not yet been repealed by the Conservative - Liberal Democrat coalition government, who seem to be reneging on their election promises, so political bloggers, activists and mainstream media journalists should all get used to living and working electronically under surveillance.

    You should help projects like Tor, as a matter of self defence against Government, Bureaucrat, Corporate and Criminal snoopers.

Open Proxy Servers

Open Proxy Servers, which allow any internet user to connect to them, typically for web browsing or for sending emails, are sometimes deliberate, and sometimes the result of mistakes or incompetence by systems administrators and software programmers.

There is a further sub-division, namely those which forward on your client PC's real IP address, and those which do not.

Typically the real IP address of your computer's internet connection is revealed by your web browser through the REMOTE_ADDR environment variable, to each and every web server you connect to.

If you are connecting via a proxy server, then it may very well reveal this IP address in the HTTP_X_FORWARDED_FOR or the HTTP_VIA environment variables.

If you visit a website, via a Proxy server, it will be the IP address of the proxy server which appears in the standard web server logfiles, however,it is often easy for a website to check and log the HTTP_VIA and HTTP_X_FORWARDED environment variables, especially if , for example, you are filling in a form with a server side script for email or account registration, for e-commerce, or to post a blog comment or discussion forum article.

Where such proxy servers have been configured not to forward the original IP address information through such environment variables, they are said to be Anonymous Proxy servers.

Although some proxy connections can be chained together, manually, many cannot, and so their use is much more error prone and more likely to betray your real IP address than using a commercial VPN service or the free Tor onion routing technique.

Various websites, e.g. http://www.freeproxy.ru, and even some commercial "anonymity" services, list or make use of **any** Open Proxy which they can find,often as a result of scanning lots of IP address ranges, to probe for such potential security weaknesses. Such lists of open proxies are constantly changing.
Some very badly configured proxy servers may actually allow access into supposedly private corporate or government intranet networks via the internet.

Some open proxies are created by privacy activists, and some are created by criminals e.g. open email proxies can be set up illegally by computer viruses to help with commercial email spam.

Many open proxies end up getting blocked by , say, the Great Firewall of China, or potentially, by the United Kingdom's British Telecom Cleanfeed system , which currently targets alleged child porn websites, at the behest of the Government, but which could, after a simple target list update, also be used for political censorship.

Other content blocking censorware systems e.g. Websense, typically installed on corporate or educational personal computers, may also block access to some open proxy servers, commercial privacy or anonymity services, and Tor exit nodes.

Tor exit nodes,which are also a form of more sophisticated open proxy, and other reported open proxies, are currently blocked by Wikipedia, not for reading, but for user registration and for editing or submission of articles - see the a
href="http://en.wikipedia.org/wiki/Wikipedia:WikiProject_on_open_proxies" target="_wpopp" title="Wikipedia:WikiProject on open proxies -new window">Wikipedia:WikiProject on open proxies

Given the massive amount of web traffic, trying to keep logfiles of proxy usage is a big, and often uneconomical task.

However, the European Union has been bounced into passing an EU Data Retention directive, which comes into force in the United Kingdom, after an 18 month delay, on 6th April 2009, after which the major upstream internet service providers will be forced to keep such lgfiles, even though they have no use for them, for at least a year, for the benefit of law enforcement and intelligence agencies, and potentially also for use in civil copyright or libel lawsuits as well.

Open proxies are a technique which can help preserve the anonymity of whistleblower sources, when communicating with investigative journalists, bloggers, and political activists, but there are risks, which you need to evaluate.

A few tips:

1. http://www.freeproxy.ru explains the various kinds of open proxy server, and publishes lists of open proxies, which are forever changing. Make your own mind up about how trustworthy any particular proxy is. Some of them on these lists are undoubtedly honeypots, designed to snoop on the possibly illegal traffic and to try to identify the users. Foreign computer crime fighters may very well not be interested in UK whistleblowers, but you cannot tell for sure.

2. You should avoid searching for open proxy servers, if you are on a corporate or government intranet, as this may flag you up as a potential whistleblower.
3. Not every open proxy server allows, encrypted SSL/TLS sessions,but those that do usually simply pass the encrypted session through unchanged (except where there is a sneaky man-in-the-middle attack in place). Therefore many open proxies do not provide any anonymity for https:// connections. Snoopers may not be able to read what content your are viewing or uploading, but they will still be able to log which websites you have visited, at what times and dates, and how much data you have uploaded or downloaded. If that amount of data is approximately the same as the size of the whistleblower document posted to a blog or forum, or sent via web email etc., then that may be sufficient circumstantial evidence to betray the identity of a whistleblower source.
4. Tor exit nodes do not always allow SSL/TLS encrypted sessions either, but since these are vital for e-commerce, many do, even behind otherwise restrictive firewalls and censorware. The Tor system will, after a short delay, find a reasonably randomly chosen exit node, which does accept SSL/TLS connection, statistically, this will usually be located outside of the United Kingdom.
5. Remember that using any SSL/TLS https:// encrypted proxy server session, or the mostly encrypted Tor proxy cloud, may protect the contents of your traffic from local snoopers, but if you have to login or otherwise authenticate to a web server or email system etc., then those details (including your real IP address) will still probably be logged by the target server, regardless of the link or session encryption, and so your whistleblower details may still be exposed, if that server is physically seized as evidence by the police or is sneakily compromised by intelligence agencies etc., either through technical hacking or bugging or by putting pressure on the systems administrators.
6. You may actually get more anonymity when using the Tor cloud by **not** using the https:// version of a web page (if there is an alternative, unencrypted version available), since all the Tor traffic is encrypted anyway between your PC and the final exit node in the Tor cloud, which will probably not be physically in the United Kingdom.
7. This applies especially to websites like the reasonably anonymous whistleblowing website wikileaks.org (based in Sweden) , which offer both http://, https:/and Tor Hidden Service methods of uploading whistleblower leak documents, but who tend to, mistakenly, insist on using https:// encryption for when someone comments on their wiki discussion pages. IWhen (not if) the wikileaks.org servers, or a blog or a discussion forum like the activist news site Indymedia UK are physically seized (this happened to IndyMedia UK at least 3 times now) , this may, in some circumstances, betray the real IP addresses of commentators with inside knowledge of a whistleblower leak i.e. suspects for a leak investigation. N.B. both wikileaks.org and IndyMedia UK claim not to log IP addresses to files, but ,inevitably, some of the recent IP address information will be available in the working memory of the machines, and their co-location hosts and upstream ISPs, will probably have some logfiles.
8. Once you have identified,or been told about, a few open web proxies, it is often fiddly and inconvenient to change your web browser settings manually. This task can be automated through the use of Firefox browser add ons such as FoxyProxy or, Torbutton
9. You can check if your open proxy server configuration is actually hiding your real IP address, via websites like Network-Tools.com

Virtual Private Networks

One useful method of increasing the security of your connections over the internet is to use a Virtual Private Network (VPN).

Many large companies and Government Departments use this technique, to tunnel an encrypted session from a home or mobile laptop computer operating in an insecure public places (such as an public WiFi hotspot or cyber café), back to a corporate network, and then via a corporate gateway, back out on to the internet.

Sometimes special client software is required e.g. from Cisco, or vendor neutral standards like an SSL/TLS web page infrastructure or IPSec can be used.

SSL/TLS web page based systems do no usually require any extra software to be installed, only a standard web browser. They might need a Client Side Digital Certificate to be installed in the browser, but this is straightforward

- There are lots of Authentication and Encryption standards and algorithms associated with VPNs. Make sure that you **disallow** any configurable options which can negotiate weak or non-existent encryption between your client PC and the VPN server. e.g. "No encryption allowed..." or "Optional encryption..." etc. to ensure that your username and password or other credentials, are never sent across the wire or by radio transmission, unencrypted in the clear.
- Use strong encryption (at least 128bit key length) , and / or a protocol which changes the encryption keys frequently. e.g. modern industry standard 802.1x authentication and AES encryption
- For extra security, do **not** store or write down your password in your Network Connection / VPN client software configurations, but **memorise** it.

  Choose a Strong Password or passphrase. As with any other web based service, like web email, if your Commercial VPN supplier offers a "Forgotten Password" or Password Recovery or Reset option, then make sure that Answers to the Challenge / Response Questions are at least as strong as your actual password e.g. if the Question is "What is your mother's maiden name ?", you usually do **not** actually have to reply **truthfully**, or with a very short , easily guessed or easily password cracked answer. US Vice-Presidential candidate Sarah Palin's Yahoo email accounts were illegally accessed in this way.

- Remember to make sure that the **Firewall software** on your PC is **aware of the new VPN IP address range**, as you will be sidestepping your usual broadband Private Internet Address e.g. 192.168.0.xxx or 192.168.1.xxx, and the built in firewall on your ADSL broadband / WiFi router (or other corporate firewall) will no longer be protecting you from various internet probes, port scans and attempts to connect to your local PC's shared disk drives and peripherals etc.

There are third party commercial companies which offer such VPN services, for a fee.

From a whistleblower source protection point of view, any of these corporate or commercial VPN services **can improve the security** of your internet connections, but they **rarely provide much extra anonymity**, as there are usually extensive log files of time and date and IP address connections to the encrypted VPN service. There will also be IP address logging and restriction policies applicable to the corporate or government system's internet gateway.

Even the commercial VPN service providers in foreign countries, some of which claim to "delete log files", etc. are not necessarily to be trusted in this regard, especially if faced with heavy legal pressure from their local law enforcement or government authorities.

Connecting via a VPN , over the public internet, through a high speed broadband connection, is often much faster than the use of dedicated dial in systems which have been used by corporate and government users for many years.

Commercial VPN services need to be paid for, and a Credit Card (or even PayPal) obviously leaves a financial audit trail back to the whistleblower or investigative journalist or blogger or political activist etc.

However, such VPN services do have their place in the arsenal of tools need to frustrate today's snoopers, especially if the company and their VPN host servers are based overseas, a technique which has been useful to, say, Chinese activists trying to evade the Great Firewall of China state censorship.

Remember that VPNs can be used in combination with other techniques, e.g.the use of Tor onion routing or open proxy servers.

We welcome reviews of such VPN services, and will update this blog post with reasonable, offshore VPN service suggestions.

- SwissVPN.net, which is based in Switzerland i.e. neither in the UK, nor the EU nor the USA, so snooping by the UK authorities might be possible, but is unlikely to be automatic, and will leave an audit trail.

  They offer a Microsoft PPTP VPN (Point to Point Tunneling Protocol) VPN service for which they charge about **$5 a month**, (credit card or PayPal payment options).

  This has the advantage that the VPN client software is already built into most Microsoft Windows operating systems (and is also available for Apple and Linux), using Microsoft's MS-CHAP2 (Challenge Handshake Authentication Protocol) authentication.

  Sometimes your internet connection's firewall may not allow the **port 1723 and type 47 IP packets** needed for GRE (Generic Routing Encapsulation), but most recent home broadband or public WiFi hotspots etc. which have **PPTP pass through**, will usually allow this.

  Some broadband routers / firewalls / WiFi access points etc. allow this ok, without displaying any user configurable options, so it is worth checking this initially with a test account first, so as not to put your real username and password credentials at risk.

  SwissVPN.net also offer, through their own free downloadable client software (not yet available for Windows Vista), the more modern EAP-TLS (Extensible Authentication Protocol) authentication, which overcomes some of the potential authentication weaknesses of MS-CHAP2, and is popular with many public and commercial WiFi hotspots.

  N.B. with either type of **authentication** the actual **encryption** of the SwissVPN.net tunnel will use 128-bit MPPE encryption (Microsoft Point-to-Point Encryption). "It uses the RSA RC4 encryption algorithm. MPPE supports 40-bit, 56-bit and 128-bit session keys, which are changed frequently to improve security. The exact frequency that the keys are changed is negotiated, but may be as frequent as every packet."

  The SwissVPN.net website includes screenshots of all of the required configuration settings, and even offers a free test account,to check if you can connect ok to their system, before purchasing any online credit.

- More VPN service suggestions or reviews are welcome

Web Browser software anonymity

Useful Firefox add-ons:

NoScript (essential protection against automatic attacks via javascript, flash etc.)

TorButton (switches to Tor browsing, but also prevents a lot snooping e.g. Browser History)

Modify Headers (control what Environment variables your web browser blabs to the world)

RequestPolicy (cross site scripting protection)

Certificate Patrol (SSL/TLS Digital Certificate checks)

Tamper Data (trace and debug the requests and responses your web browser makes with a website when you visit it or click on a button or link etc. - you will be surprised at how bloated and complicated the handshake between browser and web server can be)

For better "anonymity", you should **not** use an uncommon web browser or combination of web browser, plug-ins , add-ons, language settings etc.

See the Electronic Frontier Foundation's PanoptiClick website

http://panopticlick.eff.org/

If you do use Tor & TorButton, then your web browser settings will appear to be like those of other Tor & TorButton users, although this will emulate the most commonly seen browser log file data.

The leading Web Browser software e.g. Firefox 3. or 4 or Microsoft Internet Explorer 8 or 9 offer Private Browsing modes which can vbe set not to store or to automatically clear out Browser History and normal Cookies etc

Do not try to handle two whistleblowers at once on the same phone or email account

Do not try to handle two whistleblowers at once on the same phone or email account

It is not possible to tell if what seems to be a low level, low risk whistleblower or journalistic contact, might not develop into a high risk one in the future, once they trust you. The only professional and ethical way to conduct yourself is to to treat all of them with maximum "Moscow Rules" precautions, all of the time.

Most people would probably **never contemplate** setting up a physical face to face meeting, **to discuss confidential matters**, with **all** of their confidential whistleblower contacts at the **same place**, at the **same time**.

However, it is surprising how many journalists or bloggers etc., in contact with several confidential sources or whistleblowers at once, **risk comprising the security and anonymity of all of them**, by **sharing a phone or email address with more than one of them** i.e. if one of them gets identified (or eventually goes public), this could betray all of the others they are dealing with at the same time.

It may be acceptable to take the risk of using a shared phone number or email address for initial contacts, but do not continue to do so for more detailed contacts or for setting up physical meetings - they deserve a separate, confidential phone number or email address each.

Therefore keep a spare "whistleblowers only" mobile phone and set up some email accounts (and PGP Encryption Keys) beforehand, so that you do not arouse suspicions by suddenly obtaining these just after a whistleblower has initially contacted you.

Remember that some pre-paid mobile phone SIM cards are de-activated if they are not used after, say 6 months, and that, free Hushmail accounts need to be used at least once every 3 weeks.

If you are a whistleblower contacting a journalist etc. (or a political activist contacting a political group organiser) , then ask them if the phone number or email address that they have given you is unique to you, or if it is shared with other confidential sources, who may be currently under more investigative scrutiny than you are at present.

This works the other way for whistleblowers. They should assume that some or all of the journalists ore bloggers or elected politicians or regulatory authorities who they are initially sounding out to see if they may be interested in taking on their whistleblower story and evidence, are under various degrees of surveillance.

This may be for purposes other than that of a specific "mole hunt" or leak inquiry regarding the whistleblower's area of concern or activity.

The Communications Data Traffic Analysis which say, a leading investigative journalist will be subjected to, will reveal a list of mobile and landline phone calls (or SMS messages etc) that he receives. The next level of automated analysis will chase up each of these to see who they have been in contact with.

If your phone number or email address has been in contact with several investigative journalists etc., this will indicate suspected whistleblowing / breaches of the Official Secrets Act or commercial confidentiality etc., even if each of those contacts has not contained any incriminating details.

Therefore whistleblowers should also use individual email addresses and / or mobile phone numbers etc. for contacting each media organisation / elected politician / independent regulatory authority etc so as not to tip off their employers or other snoopers that someone is about to "blow the whistle" on something.

There is no hard and fast rule about whether to contact several potential whistleblower assistance contacts at once, or whether to try them sequentially one at a time.

Part of the problem from a whistleblower's point of view is getting anyone to listen and then getting anyone to believe their story, let alone protect their identity in the meantime, before any arrangements have been made for publication or for the secure submission of evidence.

Conclusion

Conclusion

This is not quite a comprehensive list of hints and tips to help with successful whistleblowing - do any of our astute readers have any other suitable hints and tips ?

We have kept a few techniques back (email us, using our PGP public encryption key if you want to know more).

In the UK, none of these tips really matter in a life or death way for a whistleblower, unless it is Top Secret stuff which is being passed on to a politician, journalist or blogger, but they might make it less likely that a whistleblower, or the publisher of their revelations, will be harassed by the Home Office (or other Government Department or corporation).

It is frightening that we now live in a society where the use of any of these techniques is necessary, for public interest whistleblowers to have to protect themselves with.

Further Reading

1. The Irish based Front Line Defenders charity has published Digital Security & Privacy for Human Rights Defenders manual

   We have a few minor quibbles ,but this is a very useful, clear and simple guide, which complements these hints and tips. It is of use to human rights activists living under repressive regimes, and also to UK based journalists, and political bloggers alike.

2. The United States National Security Agency does not just snoop on foreigners and US citizens, it also publishes very useful practical documentation aimed at securing US Government and Business computer systems and networks.

   Have a look at these open source Security Configuration Guides and checklists, and make sure that your computers are at least as well secured as the NSA recommendations:

   These used to be available as NSA Security Configuration Guides, but these checklists have now mostly been moved to the:

   National Institute of Standards and Technology (NIST):

   - Federal Desktop Core Configuration
   - National Checklist Program

3. The NSA also publish an illustrated, step by step guide to secure document redaction or censorship from Microsoft Word 2007 to Adobe .pdf format:

   Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word 2007 to PDF (.pdf)

4. Thomas C.Green writes in The Register about

5. Clearing swap and hibernation files properly - - probably especially important for laptop computers, which are especially vulnerable to loss or theft. See also his Windows hack for Web-surfing privacy and Internet anonymity for Windows power users gives some hints a techniques for using RAM disks rather than hard disk space for Windows and Web Browser temporary files and registry settings.
6. Privacy International:- "Legal Protections and Barriers on the Right to Information, State Secrets and Protection of Sources in OSCE Participating States" - should be read by legislators, civil servants, investigative journalists, whistleblowers and bloggers in Europe, North America and Central Asia.
7. Handbook for Bloggers and Cyber-Dissidents - March 2008 version - (2.2 Mb - 80 pages .pdf) by Reporters Without Borders
8. Reporters Guide to Covering the Beijing Olympics by Human Rights Watch.
9. Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide (.pdf - 31 pages), by the Citizenlab at the Munk Centre for International Studies at the University of Toronto.
10. Some idea of the precautions necessary for making sure that you have not been followed to clandestine physical meetings, on foot or by car, can be gleaned from this re-print of advice and techniques given to ANC / Communist activists under the South African apartheid regime - How to Master Secret Work . - *First published during the 'eighties as a series of articles in the SACP publication 'Umsebenzi'; later as a single pamphlet for underground operatives.*
11. A Practical Security Handbook for Activists and Campaigns (v 2.6) (.doc - 62 pages), by experienced UK direct action political activists (www.activistsecurity.org). It is full of practical advice, on many of the topics in this blog, including physical meetings, surveillance, anonymous letters and mobile phones. They make the point that there are private sector snoopers as well as government ones who are interested in meetings and communications between whistleblowers or activists or journalists etc.

    There is a mirror copy on this blog, in case your access to the original is blocked

    [hat tip to Mr. Tor for his suggestion in the comments below]

12. Anonymous Blogging with Wordpress & Tor - useful step by step guide with software configuration screenshots by Ethan Zuckerman at Global Voices Advocacy. (updated March 10th 2009 with the latest Tor / Vidalia bundle details)
13. Privacy International - Speaking of Terror: A survey of the effects of counter-terrorism legislation on freedom of the media in Europe (.pdf) includes sections on **Protection of journalists' sources** and materials, and **Wiretapping and surveillance of journalists** and on **Limits on Photography**.
14. The Berkman Center for Internet and Society, at the University of Harvard, in the USA,has several research projects which examine the effectiveness of State and Corporate Internet Censorship and the tools and techniques used to achieve this,m and the arms race with the Censorship Circumvention tools and techniques. They have published a useful study of some of the most popular Circumvention tools and technologies, showing their trade offs between usability, speed, security, and effectiveness at breaching the Great Firewall of China and other repressive countries.

    Unfortunately, exactly the same techniques which are useful in helping dissidents in very repressive countries, are also now needed to help to protect the anonymity of whistleblower sources and contacts with, or between, journalists, bloggers and political activists, here in the increasingly repressive United Kingdom

    2007 Circumvention Landscape Report: Methods, Uses, and Tools
    Published March 05, 2009
    Authored by Hal Roberts, Ethan Zuckerman, John Palfrey

[...]

The following tools were included in the study:

Anonymizer Anonymous Surfing - an HTTP proxy tool
Anonymizer China - an HTTP proxy tool
DynaWeb FreeGate - an HTTP proxy tool
UltraReach - an HTTP proxy tool
Circumventor / CGIProxy - a CGI proxy tool
Psiphon - a CGI proxy tool
Tor - a randomized re-routing tool
JAP - a fixed re-routing tool

Coral - a distributed hosting tool

Hamachi - a IP tunneling tool

These tools were chosen to represent most of the most popular tools and to represent a range of different technical and organizational models. There are many tools with the same or similar functionality as the tools included in the study, including Gpass, Guardian, FirePhoenix, Invisible Browsing, Metaproxy, PHPProxy, a plethora of VPN and HTTP tunneling tools, and many others.

2007 Circumvention Landscape Report: Methods, Uses, and Tools (.pdf)

15. The Crown Prosecution Service's Decision on prosecution - Mr Christopher Galley and Mr Damian Green MP is worth reading, especially the legal opinion on

    22. As already noted, Mr Galley was arrested for an alleged offence of misconduct in public office and Mr Green was arrested for an alleged offence of aiding and abetting, counselling or procuring the alleged offence by Mr Galley and of conspiring with Mr Galley for him to commit the offence of misconduct.

    23. This is not a case which falls within the framework of the Official Secrets Acts
    [...]

    This CPS Decision also mentions that

    9. The leaked document was the "Asylum and Immigration High Level Monthly Performance Report July 2007". It was marked "Restricted-Management". A copy was recovered by the police from Mr Green's Parliamentary office bearing the name "Galley" in manuscript. In his interview with the police, Mr Galley denied passing this document to anyone.
    [...]

16. Whistleblowing and Whitehall - A review of how the policies of Government Departments comply with accepted good practice on whistleblowing (.doc) - 2007 report by the Public Concern at Work whistleblowing charity.
17. This research gives an overview of internet snooping and censorship technologies, including British Telecom's CleanFeed system, and some ways in which this can be avoided, thereby preserving some whistleblower source / political dissident anonymity:

Anonymity and traceability in cyberspace (.pdf)

Richard Clayton

November 2005

Technical Report Number 653

University of Cambridge

Computer Laboratory

UCAM-CL-TR-653

ISSN 1476-2986

Dr. Richard Clayton's home pageand contact details.

18. How To Communicate Securely in Repressive Environments - a blog post with useful comments and links, and a Word (.doc) version, by Patrick Philippe Meier

House of Commons - Public Administration Committee - Tenth Report - Leaks and Whistleblowing in Whitehall - 16 July 2009

19. Public Concern at Work, together with the British Standards Institute, have produced a useful Whistleblowing Arrangements policy document for public and private sector organisations in the United Kingdom (free for individual use).

Code of Practice

In partnership with PcaW, British Standards has published a Code of Practice on whistleblowing arrangements under the classification PAS 1998/2008. PCaW is delighted that, to mark the tenth anniversary of the UK's whistleblowing regime, BSI has agreed that the Code will be available for free for individual use.

We hope you find the Code helpful. If you do, please note that PCaW has developed a range of practical support to help organisations comply with and benefit from the Code.

Copyright Provisions

Copies of this Code are available for free for individual use under licence by download from here or from www.bsigroup.com/PAS1998. For printed and own-branded copies or for a

network licence, please contact BSI at copyright@bsigroup.com.
Thank you for filling in the form:

Click here for the BSI Code of Practice. (.pdf)

20. FLOSS Manuals - Circumvention Tools - Bypassing Internet Censorship (available as a single web page for printing or as a .pdf file)

Is a neatly written and illustrated guide to to various Proxy and Virtual Private Network tools and services.

* CIRCUMVENTION TOOLS
* INTRODUCTION
* ABOUT THIS MANUAL
* BACKGROUND
* WHAT IS CIRCUMVENTION
* AM I BEING CENSORED?
* DETECTION AND ANONYMITY
* HOW THE NET WORKS
* WHO CONTROLS THE NET
* FILTERING TECHNIQUES
* FIRST TECHNIQUES
* SIMPLE TRICKS
* USING A WEB PROXY
* USING PHProxy
* USING PSIPHON
* USING PSIPHON2
* USING PSIPHON2 OPEN NODES

* RISKS
* ADVANCED TECHNIQUES
* ADVANCED BACKGROUND
* HTTP PROXIES
* INSTALLING SWITCH PROXY
* USING SWITCH PROXY
* TOR: THE ONION ROUTER
* USING TOR BROWSER BUNDLE
* USING TOR IM BROWSER BUNDLE
* USING TOR WITH BRIDGES
* USING JON DO
* TUNNELLING
* WHAT IS VPN?
* OPENVPN
* SSH TUNNELLING
* SOCKS PROXIES
* HELPING OTHERS
* INSTALLING WEB PROXIES
* INSTALLING PHProxy
* INSTALLING PSIPHON
* SETTING UP A TOR RELAY
* RISKS OF OPERATING A PROXY
* APPENDICES
* FURTHER RESOURCES
* GLOSSARY
* CREDITS

21. The Whistleblower's Handbook
How to Be an Effective Resister

Brian Martin, The Whistleblower's Handbook: How to Be an Effective Resister (Charlbury, UK: Jon Carpenter; Sydney: Envirobook, 1999). Out of print from 2008.

Entire book in pdf, 89 pages, 1.6MB

HT4W mirror copy of The Whistleblower's Handbook (.pdf)

Contents

Seven common mistakes

Seven mistakes which are commonly made

by those aiming to expose wrongdoing:

- Trusting too much
- Not having enough evidence
- Using the wrong style
- Not waiting for the right opportunity
- Not building support
- Playing the opponent's game
- Not knowing when to stop.

Leak Site Directory

From LeakDirectory

Jump to: navigation, search

Contents

[hide]

Whistle blower leaking Sites

Official and Community based sites that actively support whistle blowing / leaks about various topic

You can edit the wiki without having your ip address displayed by logging with the following Anonymous profile.

> Username: Anonymous
>
> Password: anon

You may use that template in making leak site profiles:

- Leak Site Page Template

WikiLeaks-Like Whistle blowing Sites

Leak Sites that publish leaks and accept submission of leaks, inspired by the original WikiLeaks.org concept.

- **WikiLeaks** - WikiLeaks website - love them or hate them - no new submissions for 2 years - new submission system still not launched as promised on 28/11/2011
- WikiLeaks Hrvatska (Croatia) - WikiLeaks Hrvatska website
- RevenueWatch - Revenue watch official resources and documents
- PirateLeaks CZ - PirateLeaks CZ
- Balkanleaks - Balkan Leaks website
- Indoleaks - Indoleaks website - Indonesia
- **IrishLeaks** - IrishLeaks website - uses PGP, SSL, I2P
- FrenchLeaks - FrenchLeaks website
- EnviroLeaks - EnviroLeaks website
- **RuLeaks** - Russian Leak website - uses PrivacyBox.de dropbox
- QuebecLeaks - Quebec Leak website - SSL and Tor hidden services. PGP when received.
- Jumbo Leaks - Jumbo Leaks website
- ScienceLeaks - ScienceLeaks Blogspot website
- **Filtradas** - Filtradas website - Venezuala - PGP Key and PrivacyBox.de dropbox
- Corporate Leaks - Corporate Leaks website
- **UniLeaks** - UniLeaks website - has now published a PGP key and dropped Google Analytics tracking
- **BaltiLeaks** - website Pertaining to government and business in Baltimore, Maryland, USA - PGP Key
- WikiLeaks.si - WikiLeaks.si website - Slovenia
- LeakyMails.com - LeakyMails.com website - Argentina
- MagyarLeaks - MagyarLeaks website - Hungary - PGP Key
- KHLeaks - KHLeaks website - Korea

New Concept Leak Sites

Different approaches and leaking methodologies

- **OpenLeaks** - OpenLeaks website- experienced former WikiLeaks.org tech team but not yet a live project
- Office Leaks - Office Leaks website
- IsraeliLeaks - IsraeliLeaks website
- Localeaks.com - Localeaks.com website
- TradeLeaks - TradeLeaks website
- PinoyLeaks - PinoyLeaks website
- **WikiSpooks** - WikiSpooks website- - secure and anonymous, realistically cynical and cautiously paranoid.
- MapleLeaks - MapleLeaks website
- **BritiLeaks false start** - BritiLeaks website - original false start: launched with less than no anonymity or security protection at all - see below for current site .
- **BritiLeaks** - BritiLeaks website - still to be launched, but "open alpha" testing of a secure submission system and hosting mirrors of other whistleblowing websites.
- **MurdochLeaks** - The Murdoch Leaks Project website - "will accept tips or evidence of wrong doing relating to Rupert Murdoch's affiliated institutions such as News International and News Corporation"

- OpenWatch - OpenWatch.net encourages the public to use their mobile phone software to record encounters with the police and authority, then submit them for posting online.
- LectureLeaks - LectureLeaks - Use recording mobile software to record and leak university lectures. Has content already, open source.
- **CorruptionWatch.org.za** - Corruption Watch - South Africa - Trades Union organised, anti-corruption pledge signatures, mapping of corruption hotspots, but no security or anonymity measures for contributors or informants at all except for "*Leave this field empty, if you want to stay anonymous.*"
- **100 Reporters** - 100 Reporters Whistleblower Alley - "joins 100 of the planet's finest professional reporters with whistle-blowers and citizen journalists across the globe, to report on corruption in all its forms.". Uses PrivacyBox.de (Tor and I2P) and publishes PGP Public Encryption keys
- **WCITLeaks** - WCITLeaks.org - "Bringing transparency to the ITU" - publishing leaks from the secretive United Nations - International Telecommunications Union ahead of the World Conference on International Telecommunications - SSL web form hosted on Amazon Cloud

Political Denunciation / Tip Off websites

Lunatic fringe politicians and political agenda driven mainstream media organisations sometimes try to exploit genuine public fears and worries, by running public Campaigns, to "name and shame" or to anonymously denounce locally unpopular individuals or racial or religious minorities etc.

- **MeldpuntMiddenenOostEuropeanen.nl** - Meldpunt Midden en Oost Europeanen webform - controversial "complain about Eastern European immigrants" website set up by the right wing / extremist Partij Voor de Vrijheid in the Netherlands - no encryption, no anonymity advice and no privacy policy, even though they explicitly accept "anonymous" reports and collect sensitive personal data.

Established Leak Sites

Websites which have been publishing censored or leaked material before, or independently in parallel with WikiLeaks

- **Cryptome.org** - Cryptome.org website established 1996
- **Public Intelligence** - Public Intelligence website established 2009 - now back online in Luxembourg after server move from the Netherlands caused by "complaints" to the hosting company. Good Encryption, now no longer using Quantserve web bug tracking
- SECRET OF KOREA - secret of Korea website established 2009
- LiveLeak - video leaking site established in 2006

Mainstream Media Whistle blowing Sites

Leak Sites that are operated by the media organizations directly

- **ABC News Online Investigative Unit** - ABC News Online Investigative Unit "anonymous" contact form - Australian Broadcasting Corporation - not at all secure or anonymous.

- **Al Jazeera Transparency Unit** - Al Jazeera Transparency Unit website - not very secure or anonymous - now improved
- **Radio Leaks** - Radio Sweden secure submissions website Radio Sweden is a national public service radio broadcaster
- **WSJ SafeHouse** - Wall Street Journal secure submissions website- improved since initial launch
- Austroleaks - AustroLeaks - KURIER - Investigative Recherche - mainstream newspaper based in Vienna, Austria
- **FolhaLeaks** - FolhaLeaks - Folha de S.Paulo, São Paulo, Brasil - no encryption, web form is not distinct from the main newspaper website so it betrays "anonymous" visitor details to FaceBook and to various banner advertisers etc.

Environmental Protection Whistle blowing sites

Leak Sites and Organization that accept reporting about environmental issues

- Polluters Watch - Greenpace Investigation tipline
- GreenLeaks . ORG - GreenLeaks . ORG website
- GreenLeaks . COM - GreenLeaks . COM website

National Security or Serious Crime anonymous tip off / whistleblower sites

- Australian Federal Police - Email AFP - Report a Commonwealth crime

- **Czech BIS** - Bezpečnostní Informační Služba - Security Information Service - Counter-intelligence service of the Czech Republic

- Interpol - Send message to INTERPOL

- **Mossad** - Israel Mossad Contact form (not as secure as you might expect)

- **NZ SIS** - New Zealand Security Intelligence Service Public Contribution Form - no longer uses a hidden PGP key, still tracks IP address etc. and the rest of the website still tracks visitors with Google Analytics

- Swedish Security Service - Help the Swedish Security Service

- **UK CEOP** - Child Exploitation and Online Protection Centre contact form - they now have an encrypted form to protect the Sensitive Personal Data, after a complaint to the Information Commissioner's Office
- UK Crimestoppers - UK Contact Crimestoppers Online
- **UK Home Office - CITRU** - UK Home Office - Counter Terrorism Internet Referral Unit - reporting terrorist and extremist material online - innovative secure submission progress feedback system, spoilt by use of external Google Re-Captcha
- UK Met Police Anti-Terrorist Hotline - UK London Metropolitan Police - Confidential Anti-Terrorist Hotline
- **UK Secret Intelligence Service MI6** -Secret Intelligence Service MI6 - Contact us form
- UK Security Service MI5 - UK Security Service MI5 - Reporting Suspected Threats

- UK Security Service MI5 - UK Security Service MI5 - How You Can Help - Arabic
- UK Security Service MI5 - UK Security Service MI5 - How You Can Help - Welsh

- USA Central Intelligence Agency - USA Central Intelligence Agency - English
- USA Central Intelligence Agency - USA Central Intelligence Agency - non-English
- USA Customs & Border Protection - e-allegations - - USA CBP - e-allegations - Online Trade Violation Reporting System
- USA Federal Bureau of Investigation - USA secure FBI tips and public leads submission form - see also the Financial Whistle Blowing section below

Tax Whistleblowing

- UK Government Tax Whistleblowing - UK Government Tax Whistleblowing
- USA Government Tax Whistleblowing - USA IRS Tax Whistleblowing
- Jamaica Government Tax Whistleblowing - Jamaica Government Tax Whistleblowing Hotline

Financial Whistle Blowing

- FSA - UK FSA Whistleblowing
- SFO - UK confidential international fraud reporting
- USA Securities and Exchange Commission - SEC Whistleblower Program Under Dodd-Frank Act
- EU competition commissioner - snail mail and unsecured e-mail contact details (Leniency policy unsecured FAX contact details)
- **OLAF** - European Anti-Fraud Office (OLAF) Fraud Notification System Whistleblowing and Anonymous Fraud Reporting in the European Union. (N.B. freephone telephone numbers in 27 countries)

Whistle Blowing for Censorship and Net Neutrality

- RespectMyNet - Respect MyNet, Net Neutrality abuse reporting from La Quadrature Du Net
- MobileCensorshipReporting - Mobile Censorship Reporting from Open Rights Group

Leak friendly websites

Websites which have a specific topic, audience and editorial position and as part of their reporting have frequently published high level unpublished documents

- FAS Secrecy News - USA Federation of American Scientists - Secrecy News blog established 2000 (mailinglist archive)
- Statewatch - European Statewatch website established 1991
- Global Witness - globalwitness.org
- ArmscontrolWonk - the Arms Control Wonk blog
- Metaleaks - Metaleaks Whistleblowing platforms aggregator Established in 2011, Metaleaks collects and reindex thousands of leaked documents coming from multiple sources.

Public, USA FOIA and/or historical document release sites

- USA National Security Archive The George Washington University national security archive
- USA Government Attic - FOIA focused website, includes FOIA requested records of FOIA request
- What Do They Know UK-Based FOIA request and archive site

Sites about whistleblowing and leaking

Leak Support Sites

Sites that support leaking in the editing and publishing processes, providing news, commentary or other stuff

- WLCentral - WikiLeaks Central website
- CrowdLeaks - CrowdLeaks website
- WikiLeak.org blog - WikiLeak.org blog
- CableSearch - CableSearch website
- CablegateSearch - CablegateSearch website
- Global Whistle Blog - GlobalWhistle website
- HackDemocracy - HackDemocracy Bruxelles Website
- Hints and Tips for Whistleblowers - ht4w.co.uk website - Technical Hints and Tips for protecting the anonymity of sources for Whistleblowers, Investigative Journalists, Campaign Activists and Political Bloggers etc.
- **The Whistleblower's Handbook** - The Whistleblower's Handbook (PDF 1.6MB) 89 pages - Brian Martin, The Whistleblower's Handbook: How to Be an Effective Resister
- Libreleaks.org - Libreleaks.org website
- Pistaljka - Serbian Whistleblowing Site

Sites Commenting Leaks

- Tunileaks - TunisiaLeaks website
- ThaiCables - ThaiCables website
- Rospil Russian Leaks - Rospil Russian Website

Whistle Blowing Organizations

Organizations around the world that support Whistleblowing by promoting it as a transparency practice is public and private sector.

- Transparency International Whistleblowers support website
- **SpeakUp.ie** - SpeakUp.ie - Transparency International Ireland Helpline (phone and hushmail secure dropbox)
- German Whistleblower-Netzwerk e.V.
- Whistleblowing Austria
- Canadian For Accountability NGO website
- Canadian Federal Accountability Initiative for Reform (FAIR)
- USA Official Whistleblower Protection Program website

- USA National Whistleblower Center, Government Accountability Project
- Transparency International Switzerland Whistleblowing Political Activity
- WhistleBlowing.it A Transparency International Italy WhistleBlowing Projects
- The international "publish what you pay" movement for mining, oil and other extractive industries. Supports whistle blowing through revenuewatch.org
- Global Integrity Report Open-source metrics, indicators, and techniques for assessing transparent and accountable government. Strong whistleblowing protection law considered as an effective anti-corruption framework.
- Australian Whistleblower Association
- South Africa Open Democracy Advice Center
- International Chamber of Commerce Whistleblowing Initiative
- Public Concern at Work - UK Public Concern at Work NGO and legal advice centre set up in 1993 to address public interest whistleblowing: a) confidential advice to whistleblowers b) policy & campaigning c) public education (throughout UK, and to law/policy makers and all employers)

Whistle Blowing Consulting Businesses

Organization that do business related to WhistleBlowing and leaking (Consulting, Services, Press Agency middle men etc).

- WhistleBlower Lawyers - SEC Whistleblower Attorney
- UK Whistle Blowers Press Agency Ltd - - UK Whistle Blowers Press Agency Ltd - secure Contact web form
- My Whistleblower Rights - - MyWhistleBlower Rights Confidentially report Corruption and Bribery Law Consulting

Whistle Blowing Hot Line Services

Charity and Profit organization that provide to public agencies and private corporation hotline services for whistleblowing in order to outsource the internal reporting service.

- Public Concern at Work - UK Public Concern at Work A leading authority on making public interest whistleblowing work. Provide training, consultancy, audit support and access to advice line for organisations wanting to ensure they provide their staff a real alternative to silence.
- WhistleBlow Direct - WhistleBlowing Direct Hotline service for Health Care and Social Care
- ExpoLink - Expolink Whistleblowing Hotline

Whistle Blowing Software as a Service

The commercial services are typically known as Whistleblowing reporting systems, or anonymous internet reporting systems.

- WhistleBlower Security Inc - - SaaS Whistleblower Service Look also at their Submission Interface
- UK Disclose Me - Disclose Corporate Whistle Blowing Services

- TheWatchfuli Anonymous Reporting System - TheWatchfuli Whistleblowing Services website
- MySafeWorkPlace Anonymous Reporting System - MySafeWorkPlace Whistleblowing Services website
- Swiss Corporate Whistleblowing Services and Consulting - Company Protection website
- Global Compliance SaaS phone/web whistleblowing services - Globalcompliance Website - See also their submission system (type bank to see customer list) Alert Line Whistleblowing SaaS
- Swiss Corporate Whistleblowing Services and Consulting - Company Protection website
- Disclose.com.au - Disclose.com.au Corporate Whistle Blowing Service
- ContatoSeguro.com.br - ContatoSeguro.com.br Corporate Whistle Blowing Service

Whistle Blowing Software

Software used by public and private organization to manage whistleblowing sites (We need more free software!)

- Aristotle Corporate Whistleblowing Anonymous Forum - Aristotleforum website
- ClearView Corporate Whistleblowing Software - ClearView Whistleblowing Solutions website

Open Source Whistleblowing Software

- GlobaLeaks - GlobaLeaks website - Open Source Whistleblowing Framework software project, which spawned this LeakDirectory.org wiki

- **Honest Appalachia** - Honest Appalachia website - uses Tor Hidden Service and PGP and publishes its own Open Source documents submission website software and configuration scripts to help other similar whistleblowing projects

Whistle Blowing in Corporations

A Directory of corporations that implemented corporate transparency by implementing whistleblowing through the organization:

- Italian ENI SpA Internal WhistleBlowing Result
- Netherland KLM Financial Whistleblowing Policy
- European Investment Funds Whistleblowing Policy
- European Investment Bank Whistleblowing Policy
- Anglo American Corporation SpeakUp Website

Whistle Blowing Laws, Study and Regulations

A directory of laws, study, regulations and assessments on Whistle Blowing laws and practice in various countries.

- European Parliament - Whistleblowing Rules: Best Practice; Assessment and Revision of Rules Existing in EU Institutions

- Transparency International: Alternative to Silence: Whistleblower Protection in 10 European Countries
    - Bulgaria Whistleblower Protection Assessment
    - Czech Republic Whistleblower Protection Assessment
    - Estonia Whistleblower Protection Assessment
    - Hungary Whistleblower Protection Assessment
    - Ireland Whistleblower Protection Assessment
    - Italy Whistleblower Protection Assessment
    - Latvia Whistleblower Protection Assessment
    - Lithuania Whistleblower Protection Assessment
    - Romania Whistleblower Protection Assessment
    - Slovakia Whistleblower Protection Assessment
- Australia Best Practice Whistleblowing Programs in Public Sector Organisations
- Ethics World - 18 Best Practices: The EU on Effective Whistleblowing Policies
- Japan Whistleblower Protection Act
- Switzerland Law proposal on whistleblowing in Francais, Deutsch and Italian
- Italian Laws on whistleblowing
- USA Texas Whistleblower Protection Act Attorney
- UK Public Internet Disclosure Act (whistleblowing law)
- French WhistleBlower Guideline (by Commission nationale de l'informatique)
- USA Sarbanes-Oxley Section 301: Whistleblower provisions
- UK British Standard Whistleblowing Arrangements Code of Practice
- USA Boston University: Beyond Protection - Invigorating Incentives for Sarbanes-Oxley corporate and Securities Fraud Whistleblowers
- Protecting the Whistleblowers–Asian and European Perspectives (International Anti Corruption Conference)

Whistle Blowing Cases

- USA Some Sarbanes-Oxley Whistleblowing Cases
- USA, US Qui Tam, Canada, Australia, EU Whistleblowing Cases (Caslon Analytics)

Possibly Defunct/Dead websites

- internalmemos.com Part of the fuckedcompany coverage of the internet bubble collapse. All of the 2002-2007 memos not behind the paywall are available from the internet archive highlights include:
    - MTV Europe lists anti-iraq war videos to be censored
    - MTV Europe remind everyone not to leak internal e-mails
    - US navy warns of GPS tracker Coca Cola cans
    - Steve Ballmers "realizing potential" memo
- The Memory Hole 2003-2010 project, Archive available
- Thai Leaks - Thai Leaks website
- **LocalLeaks.tk** - LocalLeaks.tk website - now blocked by .tk domain registry
- **HackerLeaks.tk** - HackerLeaks.tk website Website down as of 9 Nov 2011
- PornWikiLeaks - Porn WikiLeaks website- now points to an adult film industry job website

- blackfridaywikileaks.com - Blackfriday wikileaks America - WordPress blog with no entries since June 2011, full of Google Analytics, Quantserve etc. visitor tracking, no encryption etc.
- BrusselsLeaks - BrusselsLeaks website

Encryption / Anonymity infrastructure services/ software used by some Whistleblower Sites

- Tor - Tor project - encrypted anonymity router cloud - Tor Hidden Services and anonymised web browsing / web form submission (N.B. caveats)
- I2P - I2P - anonymous network - I2P eepsite
- PrivacyBox.de - PrivacyBox.de - encrypted contact web forms also via Tor and I2P
- Hushmail Forms - Hush Secure Forms - encrypted contact web forms
- GPG - Gnu Privacy Guard - open source Pretty Good Privacy compatible Public Key Encryption and Digital Signature cryptographic software
- TrueCrypt- TrueCrypt - open source, multi-platform file, hard disk and USB memory device etc. strong encryption
- CounterMail.com - CounterMail - encrypted email and forms, can provide free premium accounts for whistleblower sites

LeakDirectory related

Here misc stuff on Leak Directory initiative

Leak Directory backup wiki

A spam protected backup wiki mirror of this website is available at:

http://leakdirectory.wikispaces.com/