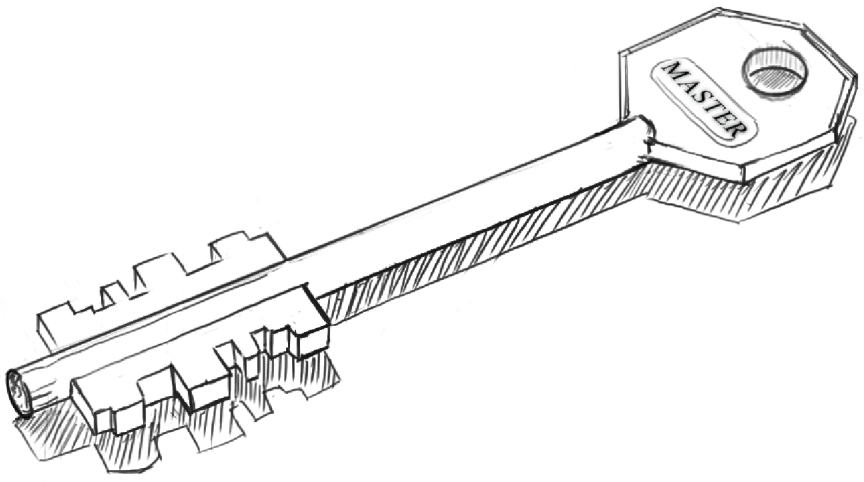
the

CryptoParty

handbook

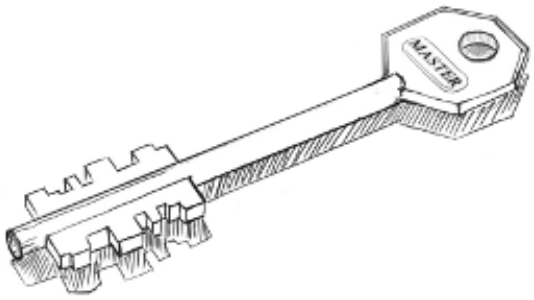


The CryptoParty Handbook

ed. Version 1

Contents

CryptoParty Handbook



A CryptoParty History: Party Like It's 1984

Because everything sounds better when someone promises there'll be beer.

What is CryptoParty?

Interested parties with computers, devices, and the willingness to learn how to use the most basic crypto programs and the fundamental concepts of their operation! CryptoParties are free to attend, public and commercially non-aligned.

CryptoParty is a decentralized, global inititative to introduce basic cryptography tools - such as the Tor anonymity network, public key encryption (PGP/GPG), and OTR (Off The Record messaging) - to the general public.

The CryptoParty idea was conceived on August 22nd 2012 as the result of a casual Twitter conversation between information activist and Twitter identity Asher Wolf and computer security experts in the wake of the Australian Cybercrime Legislation Amendment Bill 2011.

"The DIY, self-organizing movement immediately went viral, with a dozen autonomous CryptoParties being organized within hours in cities throughout Australia, the US, the UK, and Germany."

Currently sixteen CryptoParties have been held in a dozen different countries worldwide, and many more are planned. Tor usage in Australia has spiked after four CryptoParties, and the London CryptoParty had to be moved from London Hackspace to the Google campus to accomodate for the large numbers of eager participants, with 120 ticketed participants and 30 people on a wait list. Similarly, CryptoParty Melbourne found interest outstripped venue capacity - originally planned for approximately 30 participants - over 70 people turned up.

CryptoParty has received messages of support from the Electronic Frontier Foundation, AnonyOps, NSA whistleblower Thomas Drake, former Wikileaks

Central editor Heather Marsh, and Wired reporter Quinn Norton. Eric Hughes, the author of *A Cypherpunk's Manifesto* twenty years before, delivered a keynote address at Amsterdam's first CryptoParty.

A CryptoParty Manifesto

"Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth." - Oscar Wilde

version 1

In 1996, John Perry Barlow, co-founder of the Electronic Frontier Foundation, wrote 'A Declaration of the Independence of Cyberspace'. It includes the following passage:

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Sixteen years later, and the Internet has changed the way we live our lives. It has given us the combined knowlege of humankind at our fingertips. We can form new relationships and share our thoughts and lives with friends worldwide. We can organise, communicate and collaborate in ways never thought possible. This is the world we want to hand down to our children, a world with a free internet.

Unfortunately, not all of John Perry Barlow's vision has come to pass. Without access to online anonymity, we can not be free from privilege or prejudice. Without privacy, free expression is not possible.

The problems we face in the 21st Century require all of humanity to work together. The issues we face are are serious: climate change, energy crises, state censorship, mass surveillance and on-going wars. We must be free to communicate and associate without fear. We need to support opensource projects which aim to increase the commons' knowledge of technologies that we all depend on http://opensourceecology.org/wiki Contribute!

To realise our right to privacy and anonymity online, we need peer-reviewed, crowd-sourced solutions. Crypto provides the opportunity to meetup and learn how to use these solutions to give us all the means with which to assert our right to privacy and anonymity online.

- We are all users, we fight for the user and we strive to empower the user. We assert *user requests* are why computers exist. We trust in the collective wisdom of human beings, not software vendors, corporations or govern-

ments. We refuse the shackles of digital gulags, lorded over by vassal interests of governments and corporations. We are the CypherPunk Revolutionaries.

- *The right to personal anonymity, pseudonymity and privacy is a basic human right*. These rights include life, liberty, dignity, security, right to a family, and the right to live without fear or intimidation. No government, organisation or individual should prevent people from accessing the technology which underscores these basic human rights.

- Privacy is the absolute right of the individual. Transparency is a requirement of governments and corporations who act in the name of the people.

- The individual alone owns the right to their identity. Only the individual may choose what they share. Coercive attempts to gain access to personal information without explicit consent is a breach of human rights.

- All people are entitled to cryptography and the human rights crypto tools afford, regardless of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, political, jurisdictional or international status of the country or territory in which a person resides.

- Just as governments should exist only to serve their citizens - so too, cryptography should belong to the people.Technology should not be locked away from the people.

- Surveillance cannot be separated from censorship, and the slavery it entails. No machine shall be held in servitude to surveillance and censorship. Crypto is a key to our collective freedom.

- Code is speech: code is human created language. To ban, censor or lock cryptography away from the people is to deprive human beings from a human right, the freedom of speech.

- Those who would seek to stop the spread of cryptography are akin to the 15th century clergy seeking to ban the printing press, afraid their monopoly on knowledge will be undermined.

How To CryptoParty

- Throw a party. All you need is a time, a date and a location. Add it to the wiki: cryptoparty.org.

- Make sure you have Internet connectivity and enough power sources for all devices. If you do not have a place to hold a CryptoParty, find a pub or park where you can meet and squeeze the public bandwith. That will really hone your skills!

- Bring usb sticks and printed handouts for those who need them, and set up old computers for people to fiddle with and try out new skills.

- Talk about Linux to everyone you meet at your CryptoParty. If you are new to CryptoParties - ask someone "what is Linux?" ASAP.

- Make entry free for all if possible - CryptoParties are not-for-profit, not commercially aligned and especially important for those without other resources.

- Teach basic cryptographic tools to the masses. Crowd-source the best crypto. We suggest PGP, OTR, and Tor as the first tools to install.

- Invite experts and non-experts from all fields. Everyone is an expert on something.

- If you want CryptoParty to do something, start doing it. Organise organically and chaotically. ~~Have no clear leadership.~~ Urge people to take on a sudo leadership role - take a tutorial, fix the wifi, update the wiki, or organise the next CryptoParty. If someone claims others are doing it wrong - invite them to nominate themselves to do it better.

- Ask for feedback. Assimilate critics - ask them for their help in creating a better CryptoParty. Do not be scared to troll the trolls back or boot them from your space. Share feedback on the wiki. Iterate.

- A successful CryptoParty can have as many or as few as two people. Size doesn't count, it's what you do with it that matters. The criterion for success should be that everyone had fun, learned something and wants to come to the next party.

- Think of the CryptoParty movement as a huge Twitter hive ready to swarm at any moment. Tweet a lot, and make your tweets are meaningful. Re-tweet other CryptoPartiers frequently.

- Make sure the way crypto is taught at your party could be understood by a 10 year old. Then have the 10 year old teach it to an 80 year old. Breach the digital divide with random acts of awesomeness such as unfettered use of images of kittehs in all CryptoParty literature. Red underpants on heads is only mandatory if you wish to bid in our spectrum auction.

- Consider hosting private, off-the-radar CryptoParties for activists, journalists and in individuals working in dangerous locations.

- Don't scare non-technical people. Don't teach command lines before people know where the on-off buttons are located on their laptops. Everyone learns at their own pace - make sure there is support for those in need of help.

- Doing excellent stuff at CryptoParty does not require permission or an official consensus decision. If you're uncertain about the excellence of something you want to do, you should ask someone else what they think.

- Consider the need for a bouncer, particularly if your CryptoParty expects over 50 people. Dress the bouncer up as a Sumo wrestler. Do not be afraid bounce people who breach CryptoParty's anti-harrassment policy.

  CryptoParty is dedicated to providing a harassment-free sharing experience for everyone, regardless of gender, sexual orientation, disability, physical appearance, body size, heritage, or religion. Behaving like an arsehole may mean you are permanently univited to CryptoParties events. Harrassment includes:

  - hurtful or offensive comments
  - deliberate intimidation
  - direct or indirect threats
  - stalking
  - following
  - inappropriate physical contact
  - unwelcome sexual attention.

- Encourage a culture of sharing. Encourage advanced users to help not-so advanced ones. Delegate.

- Use online meeting platforms like mumble (e.g. #cryptoparty room on http://occupytalk.org/) when physical meetups are not possible or impractical.

- Copy from other cryptoparties. Remix, Reuse and Share. Create a basket of old devices people are willing to donate to more needy CryptoPartiers.

- Get the word out! Print posters and/or flyers and distribute them in you neighbourhood, post online versions to social networks and mail them to friends, for them to distribute the info even further.

- Dont sell out to sponsors for pizza and beer money. Ask people to try and bring food and drink to share. Host CryptoPicnics as often as possible. Make friends with librarians. They wield power over keys to local, public meeting rooms that may be free of charge to utilize.

- Invite all the people. Bring people together who have a wide range of skills and interests - musicians, poltical pundits, activists, hackers, programmers, journalists, artists and philsophers. Spread the love.

- Invite the graphic designers and illustrators you know to contribute new ways to help people understand crypto.

- Invite everyone to share their knowledge and their skills. Individuals with little or no coding, programming, hacking or crypto skills can change cultures by promoting the idea that privacy is a fundamental right.

- Share music, beers, & chips. Bond together over eclectic music, cheeseballs, installing GPG, Truecrypt, OTR and Tor, as well as watching movies together. We recommend Hackers, The Matrix, Bladerunner, Tron, Wargames, Sneakers, and The Net.

- Do not work too hard. Take breaks. Eat popcorn together. Create slang, phrases, memes.

- When people at CryptoParties ask for advice on "hacking the Gibson" refer them to episodes of 'My Little Pony'.

- Create fliers and advertise using slogans like: "*CryptoParties: If there is hope, it lies in the proles" and "CryptoParty like it's 1984."* CryptoParty all the things to avoid oppression and depression.

- Seed CryptoParties in your local communities - at nursing homes, scout groups, music festivals, universities, schools. Take CryptoParty to isolated and remote communties. Make friends in far away places and travel whenever possible. Ask people in rural farming communities if they'd like to CryptoParty.

- Share shimmering opportunities of crowd-sourced privacy: swap cheap, pre-paid sims, handsets and travel cards.

- Create logos in bright pink and purple, with hearts all over them. Promote CryptoParties to rebellious 13 year old girls. Declare success if rebellious 13 year old girls demand to attend your parties.

- Become friends with journalists. Invite them to your parties. Teach them crypto. ~~Do not scare them by discussing Assassination Markets.~~ stay on topic

- Strew CryptoParty sigils across your city in 3am post-party raids. Make lots of stickers, paste them everywhere. be very afraid! lives at risk!

- Experiment, constantly. ~~Do not be afraid to make mistakes.~~ Encourage people to tinker. ~~Assume all mistakes are meant to made~~. Most people under intel agency scrutiny have electronic devices already compromised before they walk in the door. Teach people to install tools from scratch, so they can do it on a new machine, away from prying eyes.

- Assume intel agencies send representative to CryptoParties. Acknowledge their presence at the start of your meeting, ask them to share their crypto skills. Joke about paranoia as often as possible without instilling panic. Wear tinfoil hats.

- Be excellent to each other and cryptoparty on.

Why Privacy Matters

Privacy is a fundamental human right which is recognized in many countries to be a central part to individual human dignity and social values, much like freedom of association and freedom of speech. Simply put, privacy is the border where we draw a line between how far a society can intrude into our personal lives.

Countries differ in how they define privacy. In the UK for example, privacy laws can be traced back to the 1300s when the English monarchy created laws protecting people from eavesdroppers and peeping toms. These regulations referred to the intrusion of a person€™s comfort and not even the King of England could enter into a poor persons house without their permission. From this perspective, privacy is defined in terms of personal space and private property. In 1880 American lawyers, Samuel Warren and Louis Brandeis described privacy as the 'right to be left alone'. In this case, privacy is synonymous with notions of solitude and the right for a private life. In 1948, the Universal Declaration of Human Rights specifically protected territorial and communications privacy which by that became part of constitutions worldwide. The European Commission on Human Rights and the European Court of Human Rights also noted in 1978 that privacy encompasses the right to establish relationships with others and develop emotional well-being.

Today, a further facet of privacy increasingly perceived is the personal data we provide to organizations, online as well as offline. How our personal data is used and accessed drives the debate about the laws that govern our behavior and society. This in turn has knock-on effects on the public services we access and how businesses interact with us. It even has effects on how we define ourselves. If privacy is about the borders which govern who we give permission to watch us and track aspects of our lives, then the amount and type of personal information gathered, disseminated and processed is paramount to our basic civil liberties.

An often heard argument, when questions of privacy and anonymity come up, goes along the lines of, "I only do boring stuff. Nobody will be interested

in it anyway" or, "I have nothing to hide". Both of these statements are easily defeated.

Firstly, a lot of companies are very interested in what boring things you do precisely so they have opportunity to offer "excellent" products fitting interests. In this way their advertising becomes much more efficient - they are able to tailor specifically to assumed needs and desires. Secondly you *do* have lots to hide. Maybe you do not express it in explicitly stated messages to friends and colleagues, but your browsing - if not protected by the techniques laid out in this book - will tell a lot about things you might rather keep secret: the ex-partner you search for using Gogle, illnesses you research or movies you watch are just few examples.

Another consideration is that just because you might not have something to hide at this moment, you may very well in future. Putting together all the tools and skills to protect yourself from surveillance takes practice, trust and a bit of effort. These are things you might not be able to achieve and configure right when you need them most and need not take the form of a spy movie. An obsessed, persistent stalker, for example, is enough to heavily disrupt your life. The more you follow the suggestions given in this book, the less impact attacks like this will have on you. Companies may also stalk you too, finding more and more ways to reach into your daily life as the reach of computer networking itself deepens.

Finally, a lack of anonymity and privacy does not just affect you, but all the people around you. If a third party, like your internet service provider, reads your email, it is also violating the privacy of all the people in your address book. This problem starts to look even more dramatic when you look at the issues of social networking websites like Facebook. It is increasingly common to see photos uploaded and tagged without the knowlege or permission of the people affected.

While we encourage you to be active politically to maintain your right to privacy, we wrote this book in order to empower people who feel that maintaining privacy on the Internet is also a personal responsibility. We hope these chapters will help you reach a point where you can feel that you have

some control over how much other people know about you. Each of us has the right to a private life, a right to explore, browse and communicate with others as one wishes, without living in fear of prying eyes.

About this book

The CryptoParty Handbook was born from a suggestion by Marta Peirano and Adam Hyde after the first Berlin CryptoParty, held on the 29th of August, 2012. Julian Oliver and Danja Vasiliev, co-organisers of the Berlin CryptoParty along with Marta were very enthusiastic about the idea, seeing a need for a practical working book with a low entry-barrier to use in subsequent parties. Asher Wolf, originator of the Crypto Party movement, was then invited to run along and the project was born.

This book was written in the first 3 days of October 2012 at Studio Weise7, Berlin, surrounded by fine food, dubious wine and a small ocean of coffee amidst a veritable snake pit of cables. Approximately 20 people were involved in its creation, some more than others, some local and some far.

The writing system, Booksprint, prioritises minimising all obstruction to expertise, making its way to the page and celebrating face-to-face discussion and dynamic task-assignment. Just like Cryptoparties themselves. The writing platform Booktype was chosen for the editing task, allowing such a tentacular feat of parallel development to happen with relative ease. Asher also opened a couple of TitanPad pages to crowdsource the Manifesto and How to CryptoParty chapters. All of it became the official Cryptoparty Handbook at the end of October the 3rd.

The Book Sprint was 3 days in length long and the full list of onsite participants included:

Adam Hyde (facilitator), Marta Peirano, Julian Oliver, Danja Vasiliev, Asher Wolf, Jan Gerber, Malte Dik, Brian Newbold, Brendan Howell, AT, Carola Hesse, Chris Pinchen with cover art (illustrations to come) by Emile Denichaud.

Make this book better here:
http://marta.free.h01.a.booktype.pro/cryptonomaton/_edit/

CryptoParty HandBook Credits

Facilitated by:
Adam Hyde

Core Team:
Marta Peirano
Asher Wolf
Julian Oliver
Danja Vasiliev
Malte Dik
Jan Gerber
Brian Newbold

Assisted by:
Brendan Howell
Teresa Dillon
AT
Carola Hesse
Chris Pinchen
'LiamO'
'l3lackEyedAngels'
'Story89'
Travis Tueffel

Cover Image
Emile Denichaud

Other material included:

https://www.flossmanuals.net/bypassing-censorship

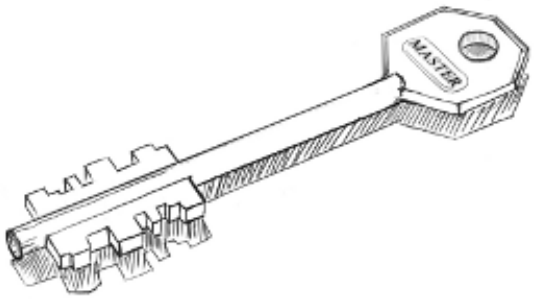
The manuals used in the second half of this book borrow from 2 books sprinted by FLOSS Manuals :

"How to Bypass Internet Censorship"2008 & 2010
Adam Hyde (Facilitator),Alice Miller,Edward Cherlin,Freerk Ohling,Janet Swisher,Niels Elgaard Larsen,Sam Tennyson,Seth Schoen,Tomas Krag, Tom

Boyle,Nart Villeneuve,Ronald Deibert,Zorrino Zorrinno, Austin Martin,Ben Weissmann,Ariel Viera,Niels Elgaard Larsen,Steven Murdoch,Ross Anderson,helen varley jamieson,Roberto Rastapopoulos,Karen Reilly,Erinn Clark,Samuel L. Tennyson, A Ravi

"Basic Internet Security" 2011
Adam Hyde (Facilitator), Jan Gerber,DanHassan,Erik Stein, Sacha van Geffen, Mart van Santen, Lonneke van der Velden, Emile den Tex and Douwe Schmidt

Email



Email

Basic Tips

Just as with other forms of communication on the web, some basic precautions always ought to be taken to ensure you have the best chance at protecting your privacy.

In brief:

- Passwords shouldn't relate to personal details and should contain a mix of more than 8 letters and other characters.
- Always be sure your connection is secure when reading email on a wireless network, especially in Internet cafes.
- Temporary files (the 'cache') on the computerthat you use to check your email can present some risks. Clear them often.
- Create and maintain separate email accounts for different tasks and interests.
- Encrypt any message you wouldn't feel comfortable sending on a post card.
- Be aware of the risks of having your email hosted by a company or organization.

Passwords

Passwords are a primary point of vulnerability in email communication. Even a secure password can be read in transit unless the connection is secure (see *HTTPS/SSL* in the glossary). In addition, just because a password is long doesn't mean it cannot be guessed by using knowledge of you and your life to determine likely words and numbers.

The general rule for creating passwords is that it should be long (8 characters or more) and have a mix of letters and other characters (numbers and symbols, which means you could just choose a short sentence). Combining your birthday with that of a family name is however a great example of how *not* to do it. This kind of information is easy to find using public resources. A popular trick is to base it on a favourite phrase and then, just to throw people off, sprinkle it with a few numbers. Best of all is to use a password generator, either on your local system or online.

Often such passwords are difficult to remember and a second point of vulnerability is opened up physical discovery. Since there is no better means of storing a password than in your own brain, services like Onlinepasswordgenerator (http://www.onlinepasswordgenerator.com/) offer a great compromise by randomly generating passwords that vaguely resemble words and present you with a list to choose from.

If you do choose to store your password outside your head, you have the choice to either write it down or use *keychain* software. This is always a risky decision, especially if the email account and password are on the same device like your phone or computer.

Keychain software, like Keepass, consolidates various passwords and passphrases in one place and makes them accessible through a master password or passphrase. This puts a lot of pressure on the master password. If you do decide to use a keychain software, remember to choose a secure password.

Finally, you should use a different password for different accounts. In that way, if one of them gets hijacked, your other accounts remain safe. Never use the same password for your work and private email accounts. See section **Passwords** to learn more about how to scure yourself.

Reading Email in Public Places

One of the great conveniences of wireless networking and 'cloud computing' is the ability to work anywhere. You may often want to check your email in an Internet cafe or public location. Spies, criminals and mischievous types are known to visit these locations in order to take advantage of the rich opportunities offered for ID theft, email snooping and hijacking bank accounts.

Here we find ourselves within an often underestimated risk of someone listening in on your communications using *network packet sniffing*. It matters little if the network itself is open or password secured. If someone joins *the same* encrypted network, s/he can easily capture and read all *unsecured* (see chapter **Secure Connection**) traffic of all of other users within the same network. A wireless key can be acquired for the cost of a cup of coffee and gives

those that know how to capture and read network packets the chance to read your password while you check your email.

Here a simple general rule always applies: if the cafe offers a network cable connection, use it! Finally, just as at a bank machine, make sure no one watches over your shoulder when you type in the password.

Cache Cunning

Here again convenience quickly paves the road to bad places. Due to the general annoyance of having to type in your password over and over again, you ask the browser or local mail client to store it for you. This is not bad in itself, but when a laptop or phone gets stolen, it enables the thief to access the owner's email account(s). The best practice is to clear this cache every time you close your browser. All popular browsers have an option to clear this cache on exit.

One basic precaution can justify you holding onto your convenient cache: disk encryption. If your laptop is stolen and the thief reboots the machine, they'll be met with an encrypted disk. It is also wise to have a screen lock installed on your computer or phone. If the machine is taken from you while still running your existing browsing session, it cannot be accessed.

Securing your communication

Whenever you write and send email in a browser or use an email program (Outlook Express, Mozilla Thunderbird, Mail.app or Mutt), you should always ensure to use encryption for the entire session. This is easily done due to the popular use of *TLS/SSL* (Secure Socket Layer) connections by email servers (**See glossary TLS/SSL**).

Https everywhere

If using a *browser* to check your email, check to see if the mail server supports SSL sessions by looking for **https://** at the beginning of the URL. If not, be sure to turn it on in your email account settings, such as Gmail or Hotmail.This ensures that not just the login part of your email session is encrypted but also the writing and sending of emails.

At the time of writing, Google's GMail uses TLS/SSL by default whereas Hot-

mail does not. If your email service does not appear to provide TLS/SSL, then it is advised to stop using it. Even if your emails are not important, you might find yourself 'locked out' of your account one day with a changed password!

When using an email program to check your email, be sure that you are using TLS/SSL in the program options. For instance in Mozilla Thunderbird the option for securing your outgoing email is found in **Tools -> Account Settings -> Outgoing Server (SMTP)** and for incoming email in **Tools -> Account Settings -> Server Settings**. This ensures that the downloading and sending of email is encrypted, making it very difficult for someone on your network, or on any of the networks between you and the server, to read or log your email.

Encrypting the email itself

Even if the line itself is encrypted using a system such as SSL, the email service provider still has full access to the email because they own and have full access to the storage device where you host your email. If you want to use a web service and be sure that your provider cannot read your messages, then you'll need to use something like *GPG* (**Appendix for GnuPG**) with which you can encrypt the email. The *header* of the email however will still contain the IP (Internet address) that the email was sent from alongside other compromising details. Worth mentioning here is that the use of *GPG* in webmail is not as comfortable as with a locally installed mail client, such as *Thunderbird* or *Outlook Express*.

Account Separation

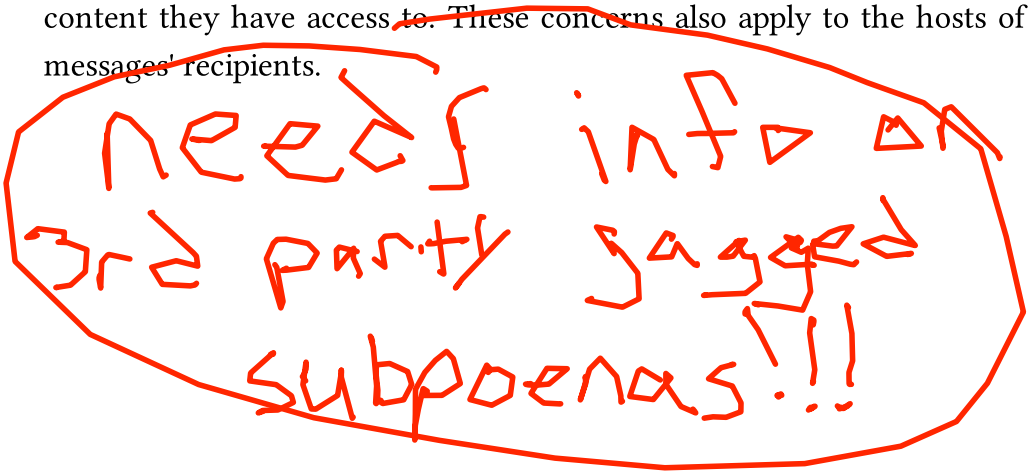
Due to the convenience of services like Gmail, it is increasingly typical for people to have only one email account. This considerably centralises the potential damage done by a compromised account. More so, there is nothing to stop a disgruntled Google employee from deleting or stealing your email, let alone Google itself getting hacked. Hacks happen.

A practical strategy is to keep your personal email, well, personal. If you have a work email then create a new account if your employers haven't already done it for you. The same should go for any clubs or organisations you be-

long to, each with a unique password. Not only does this improve security, by reducing the risk of whole identity theft, but greatly reduces the likelihood of spam dominating your daily email.

A NOTE ABOUT HOSTED EMAIL

Those that provide you with the service to host, send, download and read email are not encumbered by the use of TLS/SSL. As hosts, they can read and log your email in plain text. They can comply with requests by local law enforcement agencies who wish to access email. They may also study your email for patterns, keywords or signs of sentiment for or against brands, ideologies or political groups. It is important to read the EULA (End-user license agreement) of your email service provider and do some background research on their affiliations and interests before choosing what kind of email content they have access to. These concerns also apply to the hosts of your messages' recipients.



Email

Types of Email

The use of email almost always comes in two forms:

1. Email read, written and sent in the *browser* (webmail), or
2. Email read, written and sent using an *email program*, like Mozilla Thunderbird, Mail.App or Outlook Express.

Remotely hosted email ('webmail'), resourced using a web browser

Email sent using the *browser*, sometimes referred to as *webmail*, typically assumes an account with a remote email host like Google (Gmail), Microsoft (Hotmail) or Yahoo (Yahoo Mail). The business opportunities opened up by hosting other people's email are many: contact with other services offered by the company, brand exposure and most importantly, mining your email for patterns that can be used to evaluate your interests something of great value to the advertising industry (alongside certain Governments).

Remotely hosted email, resourced using an email program or using a web browser

Email sent using an *email program like Outlook, Thunderbird, Mail.App aso.* can also be used with a webmail service like Gmail or your company's email service. In either case, email may still be downloaded onto your computer but is retained on the email server (e.g. Gmail). Done this way, accessing email doesn't require the browser at all, but you are still using GMail, Hotmail as a service. The difference between storing email on your computer with an email program and having it stored remotely on an email server (like Hotmail, GMail or your University's service) on the Internet can appear confusing at first.

Email sent and received using an email program, not stored on the remote machine

Finally, email can also be sent to an email server but not stored there at all, merely volleyed onto its destination as soon as the email reaches the email forwarding server. Google and Microsoft do not allow for this sort of setup. Rather this is typically something your university or company will provide for you. Bear in mind that this comes with the risk of the email administrator on that system still secretly copying the email as it reaches and leaves the server.

Generally, using webmail alongisde downloading it using an email program is the best approach. This approach adds redundancy (local backups) alongside the option to delete all email from the remote server once downloaded. The latter option is ideal for content sensitive information where the possibility of account hijacking is high but risks total loss of email should the local machine go missing, without backups. Secondly, when using an email program, we have the option of using *Email Encryption* such as the popular *GPG*, something not easily set up and used with browser-only webmail services. In any case, disk encryption on the local machine is highly advisable (**AppendixDisk Encryption**).

Context considerations

You may be a server administrator yourself and run your own email service. Or your email could be stored on your company or bosses' server. Finally you may be using a service provided by a corporation, like Google (Gmail) or Microsoft (Hotmail). Each comes with its own interesting mix of considerations that relates precisely to the basic fact that unless the email *itself* is encrypted, the administrator of the email server can still secretly copy the email the moment it reaches the server. It doesn't matter that you may be using *TSL/SSL* (**Appendix SSL**) to login and check your email as this only protects the connection between your local machine and the server.

As always, if you know the risks and feel concerned it is wise to listen to them - don't send sensitive email using a service you don't trust.

Employer/Organisation

Your employer or an organisation that you are involved with is in a very good position to take advantage of your trust and read the emails of your business email account that is stored on their email server, perhaps in an effort to learn about you, your motivations, agendas and interests. Such cases of employer->employee spying are so typical they do not bear mention. ~~Your only measure against it is to use an email encryption solution like *GPG* (**Appendix GPG**).~~

Do not advocate crimes!
Also, admin may have access to your key?!

Self-administered email server

Generally speaking this is the ideal hosting configuration, but requires a higher level of technical skill. Here, in general, the risks to privacy are not only in protecting your own email against attempts at exploit (poor passwords, no SSL) but in that you have a responsibility, and perhaps a temptation, to read the emails of those you provide a service for.

not feasible.
see Bitcoinica incident!

'Free' email services

As mentioned above the risks of storing and sending your email using a service provided by a corporation are rather high if respect of your civil right to privacy is valued. The companies hosting your love letters, random expressions and diaries are always at risk of yielding to pressures from political, economic and law enforcement interests of the country to which they are legally subject. A Malaysian GMail user, for instance, risks exposing her interests and intents to a government she *did not elect*, not to mention business partners of Google interested in expanding their market reach.

Non-profit

Several non-profit web hosts offer free email accounts to organisations that are themselves non-profit or philanthropic. Some of them even offer wikis, mailing lists, chats and social networks. A consideration for organisations working in a political field may be differences of interests between the state in which the email is hosted and the political interests of the organisation using that service. Such risks would ideally be reflected in the End User License Agreement.

these orgs typically have bad sec practices!

Notes on email forwarding

Email forwarding services provide the great convenience of 'linking' one email account to another as the user sees fit. This of course is most commonly used when an account holder is on holiday and would like email forwarded from their work account to another used during travel or otherwise inaccessible outside the workplace. The risk with any external email forwarding service is the same as with remotely hosted emails through Gmail for instance: it can be copied and stored. Here email encryption using a system such as GPG (**Appendix GPG**) will ~~ensure~~ hinder that if it is copied at least it cannot be read.

Don't talk in absolutes!

Fears

Who can read the email messages that I have already sent or received?
Who can read the emails I send when they travel across the Internet?
Can the people I send emails to share them with anybody?

Emails that are sent "in the clear" without any encryption (which means the vast majority of email sent and received today) can be read, logged, and indexed by any server or router along the path the message travels from sender to receiver. Assuming you use an encrypted connection (see glossary for TLS/SSL) between your devices and your email service provider (which *everybody* should), this means in practice that the following people can still read any given message:

1. You
2. Your email service provider
3. The operators and owners of any intermediate network connections (often ambiguous multinational conglomerates or even sovereign states)
4. The recipient's email service provider
5. The intended recipient

DIAGRAM HERE?

Many webmail providers (like Gmail) automatically inspect all of the messages sent and received by their users for the purpose of showing targeted advertisements. While this may be a reasonable compromise for some users most of the time (free email!), it is disturbing for many that even their most private communications are inspected and indexed as part of a hidden and potentially very insightful profile maintained by a powerful corporate giant with a profit motive.

Additionally, somebody who can legally pressure the groups above could request or demand:

1. logged meta-data about email (lists of messages sent or received by any user, subject lines, recipients), in some juristictions even without a warrant.
2. messages sent and received by a specific user or group, with a warrant or

court order in some juristictions.
3. a dedicated connection to siphon off *all* messages and traffic, to be analyzed and indexed off site.

In cases where a user has a business or service relationship with their email provider, most governments will defend the privacy rights of the user against unauthorized and unwarranted reading or sharing of messages, though often it is the government itself seeking information, and frequently users agree to waive some of these rights as part of their service agreement. However, when the email provider is the user's employer or academic institution, privacy rights frequently do not apply. Depending on jurisdiction, businesses generally have the legal right to read all of the messages sent and received by their employees, even personal messages sent after hours or on vacation.

Historically, it was possible to "get away" with using clear text email because the cost and effort to store and index the growing volume of messages was too high: it was hard enough just to get messages delivered reliably. This is why many email systems do not contain mechanisms to preserve the privacy of their contents.Now the cost of monitoring has dropped much faster than the growth of internet traffic and large-scale monitoring and indexing of all messages (either on the sender or receiving side) is reasonable to expect even for the most innocuous messages and users. [CITE:corporate email archiving/spying, blue coat, syrian monitoring, USA utah data center, USA intercept scandals]

For more about legal protections of email messages "at rest" (technical term for messages stored on a server after having been delivered), especially regarding government access to your email messages, see:

- https://ssd.eff.org/3rdparties/govt/stronger-protection(USA)
- http://en.wikipedia.org/wiki/Data_Protection_Directive(EU)

Just like there are certain photos, letters, and credentials that you would not post "in the clear" on the Internet because you would not want that information to get indexed accidentally and show up in search results, you should never send email messages in the clear that you would not want an employer or disgruntled airport security officer to have easy access to.

Random abuse and theft by malicious hackers

What if somebody gets complete control of my email account?
I logged in from an insecure location... how do I know now if my account has been hacked?
I've done nothing wrong... what do I have to hide?
Why would anybody care about me?

Unfortunately, there are many practical, social, and economic incentives for malicious hackers to break into the accounts of random Internet individuals. The most obvious incentive is identity and financial theft, when the attacker may be trying to get access to credit card numbers, shopping site credentials, or banking information to steal money. A hacker has no way to know ahead of time which users might be better targets than others, so they just try to break into all accounts, even if the user doesn't have anything to take or is careful not to expose his information.

Less obvious are attacks to gain access to valid and trusted user accounts to collect contact email addresses from and then distribute mass spam, or to gain access to particular services tied to an email account, or to use as a "stepping stone" in sophisticated social engineering attacks. For example, once in control of your account a hacker could rapidly send emails to your associates or co-workers requesting emergency access to more secured computer systems.

A final unexpected problem affecting even low-profile email users, is the mass hijacking of accounts on large service providers, when hackers gain access to the hosting infrastructure itself and extract passwords and private information in large chunks, then sell or publish lists of login information in online markets.

NEVER send PII in clear!

Targeted abuse, harassment, and spying

Something I wrote infuriated a person in power... how do I protect myself?

If you find yourself the individual target of attention from powerful organizations, governments, or determined individuals, then some of the same techniques and principles will apply to keeping your email safe and private, but additional care must be taken to protect against hackers who might use sophisticated

techniques to undermine your devices and accounts. If a ~~hacker~~ criminal gains control of any of your computing devices or gets access to any of your email accounts, they will likely gain immediate access both to all of your correspondence, and to any external services linked to your email account.

Efforts to protect against such attacks can quickly escalate into a battle of wills and resources, but a few basic guidelines can go a long way. Use specific devices for specific communication tasks, and use them only for those tasks. Log out and shutdown your devices immediately when you are done using them. It is best to use open software encryption tools, web browsers, and operating systems as they can be publicly reviewed for security problems and keep up to date with security fixes.

Be wary of opening PDF files using Adobe Reader or other proprietary PDF readers. ~~Closed source~~ PDF readers have been known to be used to execute malign code embeded in the PDF body. If you receive a .pdf as an attachment you should first consider if you know the supposed sender and if you are expecting a document from them. Secondly, you can use PDF readers which have been tested for known vulnerabilities and do not execute code via java script. this applies to oss too!

Linux: Evince, Sumatra PDF

OS X: Preview

Windows: Evince

Use short-term anonymous throw away accounts with randomly generated passwords whenever possible.

When Encryption Goes Wrong

What happens if I lose my "keys"? Do I lose my email?

Rigorous GPG encryption of email is not without it's own problems.

If you store your email encrypted and lose all copies of your private key, you will be absolutely unable to read the old stored emails, and if you do not have a copy of your revocation certificate for the private key it could be difficult to

"prove" that any new key you generate is truly the valid one, at least until the original private key expires.

If you sign a message with your private key, you will have great difficulty convincing anybody that you did not sign if the recipient of the message ever reveals the message and signature publicly. The term for this is "non-deniability": any message you send signed is excellent evidence in court. Relatedly, if your private key is ever compromised, it could be used to read all encrypted messages ever sent to you using your public key: the messages may be safe when they are in transit and just when they are received, but any copies are a liability and a gamble that the private key will never be revealed. In particular, even if you destroy every message just after reading it, anybody who snooped the message on the wire would keep a copy and attempt to decrypt it later if they obtained the private key.

The solution is to use a messaging protocol that provides "perfect forward secrecy" by generating a new unique session key for every conversation of exchange of messages in a random way such that the session keys could not be re-generated after the fact even if the private keys were known. The OTR chat protocol provides perfect forward secrecy (http://en.wikipedia.org/wiki/-Perfect_forward_secrecy) for real time instant messaging, and the SSH protocol provides it for remote shell connections, but there is no equivalent system for email at this time.

It can be difficult to balance the convenience of mobile access to your private keys with the fact that mobile devices are much more likely to be lost, stolen, or inspected and exploited than stationary machines. An emergency or unexpected time of need might be exactly the moment when you would most want to send a confidential message or a signed message to verify your identity, but these are also the moments when you might be without access to your private keys if your mobile device was seized or not loaded with all your keys.

Email

Secure Connections

Can other people read along when I check my email?

As discussed in the Chapter **Basic Tips**, whether you use webmail or an email program you shold always be sure to use encryption for the entire session, from login to logout. This will keep anyone from spying on your communication with your email provider. Thankfully, this is easily done due to the popular use of *TLS/SSL* connections on email servers (**See appendix TLS/SSL**).

A TLS/SSL connection in the browser, when using webmail, will appear with '*https*' in the URL instead of the standard '*http*', like so:

https://gigglemail.com

If your webmail host does not provide a TLS/SSL service then you should consider discontinuing use of that account; even if your emails themselves are not especially private or important, your account can very easily be hacked by "sniffing" your password! If it is not enabled already be sure to turn it on in your account options. At the time of writing, Google's GMail and Hotmail / Microsoft Live both automatically switch your browser to using a secure connection.

If you are using an email program like Thunderbird, Mail.app or Outlook, be sure to check that you are using TLS/SSL in the options of the program. See the chapter **Setting Up Secure Connections** in the section **Email Security**.

Notes

It's important to note that the administrators at providers like Hotmail or Google, that host, receive or forward your email, can read your email even if you are using secure connections. It is also worth nothing that the private keys that Certificate Authorities sell to web site owners can sometimes end up in the hands of governments or hackers, making it much easier for a Man In The Middle Attack on connections using TLS/SSL (See Glossary for "Man in the Middle Attack"). An example is here, implicating America's NSA and several email providers: http://cryptome.info/0001/nsa-ssl-email.htm

We also note here that a *Virtual Private Network* is also a good way of securing your connections when sending and reading email but requires using a *VPN* client on your local machine connecting to a server. See the chapter **Virtual Private Networking** in the **Browsing** section.

Secure Message

It is possible to send and receive secure email using ~~standard~~ current email programs by adding a few add-ons. The essential function of these addons is to make the message body (but not the To:, From:, CC: and Subject: fields) unreadable by any 3rd party that intercepts or otherwise gains access to your email or that of your conversation partner. This process is known as *encryption.*

Secure email is generally doneusing a technique called *Public-Key Cryptography*. Public-Key Cryptography is a clever technique that uses two code keys to send a message. Each user has a *public key*, which can only be used to encrypt a message but not to decrypt it. The public keys are quite safe to pass around without worrying that somebody might discover them. The *private keys* are kept secret by the person who receives the message and can be used to decode the messages that are encoded with the matching public key.

In practice, that means if Rosa wants to send Heinz a secure message, she only needs his public key which encodes the text. Upon receieving the email, Heinz then uses his private key to decrypt the message. If he wants to respond, he will need to use Rosa's public key to encrypt the response, and so on.

What software can I use to encrypt my email?

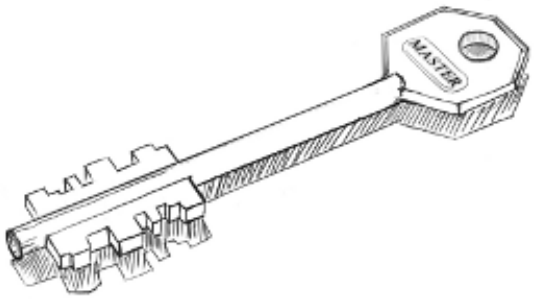
The most popular setup for public-key cryptography is to use *Gnu Privacy Guard* (GPG) to create and manage keys and an add-on to integrate it with standard email software. Using GPG will give you the option of encrypting sensitive mail and decoding incoming mail that has been encrypted but it will not force you to use it all the time. In years past, it was quite difficult to install and set up email encryption but recent advances have made this process relatively simple.

See section **Email Encryption** for working with GPG in the scope of your operating system and email program.

If you use a *webmail* service and wish to encrypt your email this is more difficult. You can use a GPG program on your computer to encrypt the text using your public key ~~or you can use an add-on, like *Lock The Text* (http://lockthetext.sourceforge.net/).~~ If you want to keep your messages private, we suggest using a dedicated email program like Thunderbird instead of webmail.

do not suggest people use browser ext that makes key data or sig oracles available!!!

Browsing



Basic Tips

In Brief

- When you visit a website you give away information about yourself to the site owner, unless precautions are taken.
- Your browsing on the Internet may be tracked by the sites you visit and partners of those sites. Use anti-tracking software.
- Visiting a website on the Internet is never a direct connection. Many computers, owned by many different people are involved. Use a secure connection to ensure your browsing can not be recorded.
- What you search for is of great interest to search providers. Use search anonymising software to protect your privacy.
- It is wiser to trust Open Source browsers like Mozilla Firefox as they can be more readily security audited.

Your browser talks about you behind your back

All browsers communicate information to the web server serving you a web page. This information includes name and version of the browser, referral information (a link on another site, for instance) and the operating system used.

Websites often use this information to customise your browsing experience, suggesting downloads for your operating system and formatting the web page to better fit your browser. Naturally however, this presents an issue as regards the user's own anonymity as this information becomes part of a larger body of data that can be used to identify you individually.

Stopping the chatter of your browser is not easily done. You can, however, falsify some of the information sent to web servers while you browse by altering data contained in the *User Agent*, the browser's identity. There is a very useful plugin for Firefox, for instance, called *User Agent Switcher* that allows you to set the browser identity to another profile selected from a drop down list of options.

Web sites can track you as you browse

Small files, called *cookies*, are often written onto your computer by web sites. Cookies present certain conveniences, like caching login data, session information and other data that makes your browsing experience smoother. These small pieces of data however present a significant risk to your right to anonymity on the web as they can be used to identify you if you return to a site and also to track you as you move from site to site. Coupled with the User Agent, they present a powerful and covert means of remotely identifying your person.

The ideal solution to this problem is to deny all website attempts to write cookies onto your system but this can greatly reduce the quality of your experience on the web.

See the section **Tracking** for guides as to how to stop web servers tracking you.

Searching online can give away information about you

When we search online using services like Bing or Google our right to privacy is already at risk, vastly more so than asking a person at an Information Desk in an airport, for instance.

Combined with the use of cookies and User Agent data this information can be used to build an evolving portrait of you over time. Advertisers consider this information very valuable, use it to make assumptions about your interests and market you products in a targeted fashion.

While some customers may sing the praises of targeted advertising and others may not care, the risks are often misunderstood. Firstly, the information collected about you may be requested by a government, even a government you did not elect (Google, for instance, is an American company and so must comply with American judicial processes and political interests). Secondly there is the risk that merely searching for information can be misconstrued as intent or political endorsement. For instance an artist studying the aesthetics of different forms of Religious Extremism might find him or herself in danger of being associated with support for the organisations studied. Finally there is

the risk that this hidden profile of you may be sold on to insurance agents, provided to potential employers or other customers of the company whose search service you are using.

Even once you've ensured your cookies are cleared, your *User Agent* has been changed (see above and chapter **Tracking**) you are still giving away one crucial bit of information: the Internet Address you are connecting from (see chapter **What Happens When You Browse**). To avoid this you can use an anonymising service like *Tor* (see chapter **Anonymity**). If you are a Firefox user (recommended) be sure to install the excellent *Google Sharing* addon, an anonymiser for Google search. Even if you don't consciously use Google, a vast number of web sites use a customised Google Search bar as a means of exploring their content.

With the above said, there are no reasons to trust Google, Yahoo or Bing. We recommend switching to a search service that takes your right to privacy seriously: DuckDuckGo (http://duckduckgo.com/).

More eyes than you can see

The Internet is a big place and is not one network but a greater network of many smaller interconnected networks. So it follows that when you request a page from a server on the Internet your request must traverse many machines before it reaches the server hosting the page. This journey is known as a *route* and typically includes at least 10 machines along the path. As packets move from machine to machine they are necessarily copied into memory, re-written and passed on.

Each of the machines along a network route belongs to someone, normally a company or organisation and may be in entirely different countries. While there are efforts to standardise communication laws across countries, the situation is currently one of significant jurisdictional variation. So, while there may not be a law requiring the logging of your web browsing in your country, such laws may be in place elsewhere along your packet's route.

The only means of protecting the traffic along your route from being recorded or tampered with is using *end to end encryption* like that provided by

TSL/Secure Socket Layer (**See chapter Encryption**) or a Virtual Private Network (**See chapter VPN**).

Your right to be unknown

Beyond the desire to minimise privacy leakage to specific service providers, you should consider obscuring the Internet Address you are connecting from more generally (see chapter **What Happens When You Browse**). The desire to achieve such anonymity spurred the creation of the *Tor Project*.

Tor uses an ever evolving network of nodes to route your connection to a site in a way that cannot be traced back to you. It is a very robust means of ensuring your Internet address cannot be logged by a remote server. See the chapter **Anonymity** for more information about how this works and how to get started with Tor.

Fears

Socal Networking - what are the dangers?

The phenomenon of Internet based Social Networking has changed not just how people use the Internet but its very shape. Large data centers around the world, particularly in the US, have been built to cater to the sudden and vast desire for people to upload content about themselves, their interests and their lives in order to participate in Social Networking.

Social Networking as we know it with FaceBook, Twitter (and earlier Myspace) are certainly far from 'free'. Rather, these are businesses that seek to develop upon, and then exploit, a very basic anxiety: the fear of social irrelevance. As social animals we can't bear the idea of missing out and so many find themselves placing their most intimate expressions onto a businessman's hard-disk, buried deep in a data center in another country - one they will never be allowed to visit.

Despite this many would argue that the social warmth and personal validation acquired through engagement with Social Networks well out-weighs the potential loss of privacy. Such a statement however is only valid when the *full* extent of the risks are known.

The risks of Social Networking on a person's basic right to privacy are defined by:

The scope and intimacy of the user's individual contributions.

- A user posting frequently and including many personal details constructs a body of information of greater use for targetted marketing.

The preparedness of the user to take social risks.

- A user making social connections uncritically is at greater risk from predators and social engineering attacks.

The economic interests and partners of the organisation providing the service.

- Commissioned studies from clients, data mining, sentiment analysis.

Political/legal demands exerted by the State against the organisation in the jurisdiction(s) in which it is resident.

- Court orders for data on a particular user (whether civilian or foreigner).
- Surveillance agendas by law enforcement or partners of the organisation.
- Sentiment analysis: projections of political intent.

With these things in mind it is possible to chart a sliding scale between projects like Diaspora and Facebook: the former promises some level of organisational transparency, a commitment to privacy and a general openness, whereas Facebook proves to be an opaque company economically able to gamble with the privacy of their users and manage civil lawsuits in the interests of looking after their clients. As such there is more likelihood of your interactions with a large Social Network service affecting how an Insurance company or potential employer considers you than a smaller, more transparent company.

Who can steal my identity?

This question depends on the context you are working within as you browse. A weak and universal password presents a danger of multiple services from Social Networking, Banking, WebMail etc being account hijacked. A strong and universal password on a wireless network shared with others (whether open or encrypted) is just as vulnerable. The general rule is to ensure you have a strong password (see section on **Passwords**).

Wireless networks

Here we find ourselves amidst an often underestimated risk of someone listening in on your communications using *network packet sniffing*. It matters little if the network itself is open or password secured. If someone uses the same encrypted network, he can easily capture and read all unsecured traffic of other users within the same network. A wireless key can be acquired for the cost of a cup of coffee and gives those that know how to capture and read

network packets the chance to read your password while you check your email.

A simple rule always applies: if the cafe offers a network cable connection, use it! Finally, just as at a bank machine, make sure no one watches over your shoulder when you type in the password.

The browser cache

Due to the general annoyance of having to type in your password repeatedly, you allow the browser or local mail client to store it for you. This is not bad in itself, but when a laptop or phone gets stolen, this enables the thief to access the owner's email account(s). The best practice is to clear this cache every time you close your browser. All popular browsers have an option to clear this cache on exit.

One precaution can justify you holding onto your convenient cache: disk encryption. If your laptop is stolen and the thief reboots the machine, they'll be met with an encrypted disk. It is also wise to have a screen lock installed on your computer or phone. If the machine is taken from you while still running your existing user session, it cannot be accessed.

Securing your line

Whenever you log into any service you should always ensure to use encryption for the entire session. This is easily done due to the popular use of *TSL/SSL* (Secure Socket Layer).

Check to see the service you're using (whether EMail, Social Networking or online-banking) supports TSL/SSL sessions by looking for **https://** at the beginning of the URL. If not, be sure to turn it on in any settings provided by the service. To better understand how browsing the World Wide Web works, see the chapter **What Happens When I Browse?**

Can I get in trouble for Googling weird stuff?

Google and other search companies may comply with court orders and warrants targeting certain individuals. A web site using a customised Google Search field to find content on their site may be forced to log and supply all search queries to organisations within their local juristiction. Academics, artists and researchers are particularly at risk of being misunderstood, assumed to have motivations just by virtue of their apparent interests.

Who is keeping a record of my browsing and am I allowed to hide from them?

It is absolutely within your basic human rights, ~~and commonly constitutionally protected,~~ to visit web sites anonymously. Just as you're allowed to visit a public library, skim through books and put them back on the shelf without someone noting the pages and titles of your interest, you are free to browse anonymously on the Internet.

How to not reveal my Identity?

See the chapter on **Anonymity**.

How to avoid being tracked?

See the chapter on **Tracking**.

What happens when you browse

Browsing the web is communicating. You might not send as much text in terms of number of words, but it is always the browser which initiates and maintains the communication by requesting the bits and pieces which are woven into what is eventually displayed on your screen.

Browsers like Mozilla Firefox, Google Chrome, Opera, Safari & Internet Explorer all work in a similar manner. When we type a URL (e.g. "http://happybunnies.com") in the adress bar, the browser requests the website (which is just a special kind of text) from a remote server and then transforms it into colored blocks, text and images to be displayed in the browser window. To see the text the way the browser sees it, one just has to click on the *View --> Page source* menu entry in the browser. What comes up is the same webpage but in HTML a language mainly concerned with content, context and links to other resources (CSS and JavaScript) which govern the way these contents are displayed and behave.

When the browser tries to open a webpage and assuming there are no proxies involved the first thing it does is to check its own cache. If there is no past memories of such website, it tries to resolve the name into an address it can actually use. It is an internet program, so it needs an Internet Protocol address (IP address or just IP). To get this address it asks a DNS Server (kind of a telephone book for internet programs) which is installed in the router of your internet access by default. The IP address is a numerical label assigned to every device in the (global) network, like the address of a house in the postal system and as the address of your home, you should be very careful to whom you hand out the IP address you are browsing from (by default this is: to everyone). Once the IP address has been received, the browser opens a TCP (just a communication protocol) connection to the destination host and starts sending packages to a port at this address (typically no. 80 (ports are like doors to the servers, there are many but usually only a few are open) unless another path is specified. These packages travel through a number of servers on the internet (up to a couple of dozens depending on were the target address is located). The server then looks for the requested page and, if found,

delivers it using the HTTP protocol. (To prevent others from reading or altering the data, TLS/SSL can be used to below HTTP to secure the connection)

When the HTTP response arrives, the browser can close the TCP connection or reuse it for subsequent requests. The response can be one of many things, from some sort of redirection or a classic Internal Server Error (500). Provided the response proceeds as expected the browser will store the page in a cache for further use, decode it (uncompress it if compressed, rendered if video codec, etc) and display/play it according to instructions.

Now, the process can be illustrated in a little conversation between browser (B) and server (S):

B: "Hallo."

S: "Hey!"

B: "May I get that page with the happy bunnies, please?"

S: "Well, here you are."

B: "Oh, maybe you could also give me a big version of that picture of that bunny baby cuddling a teddy bear."

S: "Sure, why not."

[...]

B: "That's all for now. Thank you. Bye."

Note that there are lots of activities happening parallel to this TCP/IP exchange. Depending on how you have configured its options, your browser might be adding the page to browser history, saving cookies, checking for plugins, checking for RSS updates and communicating with a variety of servers, all while you're doing something else.

A topography of you: footprints

Most important: you will leave footprints. Some of them will be left on your

own computer a collection of cache data, browsing history and naughty little files with elephantic memory called cookies. They are all very convenient; speed up your browser's performance, reduce your data download or remember your passwords and preferences from Social Networks. They also snitch on your browsing habits and compile a record of everywhere you go and everything you do there. This should bother you if you are using a public computer station at a library, work at a cybercafe, or share your appartment with a nosey partner!

Even if you configure your browser to not keep a history record, reject cookies and delete cached files (or allocate zero MB of space for the cache), you would still leave breadcrumbs all over the Internet. Your IP address is recorded by default everywhere, by everyone and the packets sent are monitored by an increasing number of entities - commercial, governmental or criminal, along with some creeps and potential stalkers.

Democratic goverments everywhere are redesigning regulations to require Internet providers to keep a copy of everything so they can have later access to it. In the USA, section 215 of the American PATRIOTact *'prohibits an individual or organization from revealing that it has given records to the federal government, following an investigation*'. That means that the company you pay every month as a customer to provide you with Internet access can be ordered to turn over your browsing and email records without your knowledge.

Most of the time though, surveillance is not a *1984* affair. Google collects your searches along with your browser identification (*user agent*), your IP and a whole bunch of data that can eventually lead to your doorstep, but the ultimate aim is usually not political repression, but market research. Advertisers don't fuss about advertising space any more, they just want to know everything about you. They want to know your dietary and medication habits, how many children you have and where you take them on holidays, how you make your money, how much you earn, and how you like to spend it. Even more: they want to know how you *feel* about stuff. They want to know if your friends respect those feelings enough so that you can convince them to change *their* consumption habits. This is not a conspiracy, but rather the nature of Information Age capitalism. To paraphrase a famous observa-

tion of the current situation, the best minds of our generation are thinking about how to make people click ads.[4]

Some people think ads can be ignored or that having advertisers cater for our specific needs is a win-win situation, because at least they are spammed with things they may actually want. Even if that was the case ~~(it isn't)~~: should we trust Google with such intimate details of our life? Even if we trust Google to 'do no evil', it can still be bought by someone we do not trust; benevolentLarry Page andSergey Brin could be overruled by their own Board, or their data base be sequestered by a fascistic goverment. One of their 30,000 employees worldwide could cut loose and run with our data. Their servers can be hacked. And in the end, they are just interested in their customers, *the companies paying for advertising*. We are just the product being sold.

Moreover; in the Social Networks our browsing habits are generating a ~~P~~ermanent ~~R~~ecord, a collection of data so vast that the information that Facebook keeps about a given user alone can fill 880 pages. Nobody will be surprised to learn that Facebook's purpose is not to make us happy again: if you are not paying for it, you're not the customer, you're the product. But even if you don't care about their commercial goals, consider this: the platform has publicly admitted hackers break into hundreds of thousands of Facebook accounts every day.

For a taste of what lurks behind the curtains of the websites you visit, install a plugin/add-on called *Ghostery* to your browser. It's like an x-ray-machine which reveals all the surveillance technology which might be (and often *is*) embedded in a web page, normally invisible to the user. In the same line, *Do Not Track Plus* and *Trackerblock* will give you further control over online tracking, through cookie blocking, persistent opt-out cookies, etc. Our following chapter *Tracking* will equip you with expertise in such topics.

Do not track is a request that can't be tracked!

Even in between your computer and the router, your ~~packages~~ packets can easily be intercepted by anyone using the same wireless network in the casual enviroment of a cafe. It is a jungle out there, but still we choose passwords like "password" and "123456", perform economic transactions and buy tickets on public wireless networks and click on links from unsolicited emails. It is not only our right to preserve our privacy but also our responsibility to defend

that right against the intrusions of goverments, corporations and anyone who attempts to disposses us. If we do not exercise those rights today, we deserve whatever happens tomorrow.

---

1. If you are a Unix user, you can use the tcpdump command in the bash and view real time dns traffic. It's loads of fun! (and disturbing)
2. See list of TCP and UDP port numbers(http://en.wikipedia.org/wiki/-List_of_TCP_and_UDP_port_numbers)
3. If this exchange is happening under an HTTPS connection, the process is much more complicated and also much safer, but you will find out more about that in a most fascinating chapter called Encryption.
4. *This Tech Bubble Is Different(http://www.businessweek.com/magazine/-content/11_17/b4225060960537.htm)*, Ashlee Vance (Businessweek magazine)

Consider removing/ revamping this whole section. No useful info + lots of conjecture!

most useful topics are repeated below under tracking!

Accounts and Security

When you browse, you may be logged into various services, sometimes at the same time. It may be a company website, your email or a social networking site. Our accounts are important to us because highly sensitive information about us and others is stored on machines elsewhere on the Internet.

Keeping your accounts secure requires more than just a strong password (see section *Passwords*) and a secure communication link with the server via TLS/SSL (see chapter *Secure Connection*). Unless specified otherwise, most browsers will store your login data in tiny files called *cookies*, reducing the need for you re-type your password when you reconnect to those sites. This means that someone with access to your computer or phone may be able to access your accounts without having to steal your password or do sophisticated snooping.

As smart phones have become more popular there has been a dramatic rise in account hijacking with stolen phones. Laptops theft presents a similar risk. If you do choose to have the browser save your passwords then you have a few options to protect yourself:

- Use a screen lock. If you have a phone and prefer an unlock pattern system get in the habit of wiping the screen so an attacker can not guess the pattern from finger smears. On a Laptop, you should set your screensaver to require a password as well as a password on start-up.
- Encrypt your hard disk. TrueCrypt is an open and secure disk encryption system for Windows 7/Vista/XP, Mac OS X and Linux. OSX and most Linux distributions provide the option for disk encryption on install.
- Android Developers: do not enable USB debugging on your phone by default. This allows an attacker using the Android *adb shell* on a computer to access your phone's hard disk without unlocking the phone.

Can malicious web sites take over my accounts?

Those special cookies that contain your login data are a primary point of vulnerability. One particularly popular technique for stealing login data is called *click-jacking*, where the user is tricked into clicking on a seemingly innocuous link, executing a script that takes advantage of the fact you are logged in. The login data can then be stolen, giving the remote attacker access to your account. While this is a very complicated technique it has proven effective on several occassions. Both Twitter and Facebook have seen cases of login sessions being stolen using these techniques.

It's important to develop a habit for thinking before you click on links to sites while logged into your accounts. One technique is to use another browser entirely that is not logged into your accounts as a tool for testing the safety of a link. Always confirm the address (URL) in the link to make sure it is spelled correctly. It may be a site with a name very similar to one you already trust. Note that links using URL shorteners (like http://is.gd and http://bit.ly) present a risk as you cannot see the actual link you are requesting data from.

If using Firefox on your device, use the add-on NoScript http://noscript.net as it mitigates many of the *Cross Site Scripting* techniques that allow for your cookie to be hijacked but it will disable many fancy features on some web sites.

Tracking

When you browse the web tiny digital traces of your presence are left behind. Many web sites harmlessly use this data to compile statistics and see how many people are looking at their site and which pages are popular, but some sites go further and use various techniques to track individual users, even going as far as trying to identify them personally. It doesn't stop there ~~however~~. Some firms store data in your web browser which can be used to track you on other web sites. This information can be compiled and passed on to other organizations without your knowledge or permission.

This all sounds ominous but really who cares if some big company knows about a few web sites that we have looked at? Big web sites compile and use this data for "behavioral advertising" where ads are tailored to fit your interests exactly. That's why after looking at, say, the Wikipedia entry for Majorca, one may suddenly start seeing lots of ads for packaged vacations and party hats. This may seem innocent enough, but after doing a search for "Herpes Treatments" or "Fetish Communities" and suddenly seeing listings for relevant products, one may start to feel that the web is getting a bit too familiar.

Such information is also of interest to other parties, like your insurance company. If they know you have been looking at skydiving sites or forums for congenital diseases, your premiums may mysteriously start going up. Potential employers or landlords may turn you down based on their concerns about your web interests. In extreme instances, the police or tax authorities may develop an interest without you ever having committed a crime, simply based on suspicious surfing.

How do they track us?

Every time you load a web page, the server software on the web site generates a record of the page viewed in a log file. This is not always a bad thing. When you log in to a website, there is a need for a way to establish your identity and keep track of who you are in order to save your preferences, or present you with customized information. It does this by passing a small file to your browser and storing a corresponding reference on the web server. This file is called a *cookie*. It sounds tasty but the problem is that this information stays on your computer even after leaving the web site and may phone home to tell the owner of the cookie about other web sites you are visiting. Some major sites, like Facebook and Google have been caught using them to keep track of your browsing even after you have logged out.

Supercookies / Evercookie / Zombie Cookies?

How can I prevent tracking?

The simplest and most direct way to deal with tracking is to delete the cookie files in your browser:

[show how in Firefox (tools->Clear Recent History...), chrome, IE, etc.]

The limitation to this approach is that you will receive new cookies as soon as you return to these sites or go to any other pages with tracking components. The other disadvantage is that you will lose all of your current login sessions for any open tabs, forcing you to type in usernames and passwords again. A more convenient option, supported by current browsers is *private browsing* or *incognito mode*. This opens a temporary browser window that does not save the history of pages viewed, passwords, downloaded files or cookies. Upon closing the private browsing window, all of this information is deleted. You can enable private browsing:

[show how in Firefox (tools->Start Private Browsing), chrome, IE, etc.]

This solution also has it's limitations. We cannot save bookmarks, remember passwords, or take advantage of much of convenience offered by modern browsers. Thankfully, there are several plugins specially designed to address

the problems of tracking. The most extensive, in terms of features and flexibility, is Ghostery. The plugin allows you to block categories or individual services that track users. Here's how you install Ghostery:

[screenshots here installing the plugin]

Another option is to install an ad-blocking plugin like AdBlockPlus. This will automatically block many of the tracking cookies sent by advertising companies but not those used by Google, Facebook and other web analytics companies. [expand on this maybe, explain "web analytics"]

How can I see who is tracking me?

The easiest way to see who is tracking you is to use the Ghostery plugin. There is a small icon on the upper right or lower right corner of your browser window that will tell you which services are tracking you on particular web sites.

{ Suggestion: Add Abine.com's Do Not Track add-on. I suggest using both Ghosterly and DNT, as occasionally they block a different cookie. Abine also has Privacy Suite, recently developed which can give a proxy telephone and proxy email, similar to 10 Minute Mail or Guerilla Mail for fill- in emails for forms. } DNT can itself be tracked!

A word of warning.

If you block trackers, you will have a higher level of privacy when surfing the net. However, government agencies, bosses, hackers and unscrupulous network administrators will still be able to intercept your traffic and see what you are looking at. If you want to secure your connections you will need to read the chapter on encryption. Your identity may also be visible to other people on the internet. If you want to thoroughly protect your identity while browsing, you will need to take steps toward online anonymity which is explained in another section of this book. Which?

Anonymity

Intro

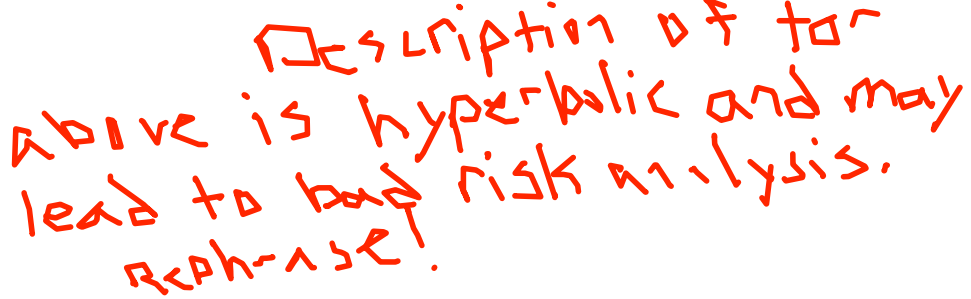
Article 2 of the Universal Declaration of Human Rights states:

"Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.".

One way of enforcing this basic right in hostile environments is by means of anonymity, where attempts to connect an active agent to a specific person are blocked.

Acting anonymously is also a great way to help others with a high need for protection the bigger the herd of sheep, the harder it is to target a specific one. An easy way to do so is by using TOR, a technique which routes internet traffic between users of a special software, thus making it untraceable to any specific IP address or person without having control over the whole network (and nobody has that yet in the case of the internet). A highly functional means to protect ones own identity is by using anonymous proxy servers and Virtual Private Networks (VPN).



Proxy

*"An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable. It is a proxy [server] computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information." (http://en.wikipedia.org/wiki/Anonymizer)*

This provides no protection and leaves your privacy completely in the hands of the operator

The main purpose behind using a proxy is to hide or to change Internet address (IP address) assigned to user's computer. There can be a few reasons for needing to do so, for example:

- To anonymize access to particular server(s) and/or to obfuscate traces left in the log files of a web-server. For instance a user might need/want to access sensitive materials online (special materials, research topics or else) without triggering authorities attention.
- To break throughfirewalls of corporations or repressive regimes. A corporation/government can limit or completely restrict Internet access for a particular IP address or a range of IP addresses. Hiding behind a proxy will help to trick these filters and access otherwise forbidden sites.
- To watch online video and streams banned in your country due to legal issues.
- To access websites and/or materials available only for IP addresses belonging to a specific country. For example, a user wants to watch a BBC video stream (UK-only) while not residing in the UK.
- To access the Internet from a partially banned/blocked IP address. Public IP addresses can often have "bad reputation" (bandwidth abuse, scam or unsolicited email distribution) and be blocked by some web-sites and servers.

While a usual scenario would be to use proxy for accessing the Web (HTTP), practically Internet protocol can be proxied - i.e. sent via a remote server. Unlike a router, proxy server is not directly forwarding remote user requests but rather mediates those requests and echos responses back to remote user's computer.

Proxy (unless setup as "transparent") does not allow direct communication to

the Internet thus applications such as browsers, chat-clients or download applications need to be made aware of the proxy server (see *Safer Browsing/Proxy settings* chapter)

Tor

"- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android."
(https://www.torproject.org)

Tor is a system intended to enable online anonymity, composed of client software and a network of servers which can hide information about users' locations and other factors which might identify them. Imagine a message being wrapped in several layers of protection: every server needs to take off one layer, thereby immediately deleting the sender information of the previous server.

Use of this system makes it more difficult to trace Internet traffic to the user, including visits to Web sites, online posts, instant messages, and other communication forms. It is intended to protect users' personal freedom, privacy, and ability to conduct confidential business, by keeping their internet activities from being monitored. The software is open-source and the network is free of charge to use.

Tor cannot and does not attempt to protect against monitoring the traffic entering and exiting the network. While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation). *End-to-End Correlation* is a way of matching an online identity with a real person.

A recent case of this involved the FBI wanting to prove that the man Jeremy Hammon was behind an alias known to be resonsible for several Anonymous attacks. Sitting outside his house, the FBI were monitoring his wireless traffic alongside a chat channel the alias was known to visit. When Jeremy went on-

line in his apartment, inspection of the wireless packets revealed he was using Tor at the same moment the suspected alias associated with him came online in the surveilled chat channel. This was enough to incriminate Jeremy and he was arrested.

See section *Safer Browsing/Using Tor* for setup instructions.

VPN

The way your data makes it to the desired server and back to your laptop computer or a mobile device is not as straightforward as it might first seem. Say, you are connected to a wireless network at home and opening a wikipedia.org page. The path your request (data) takes will consist of multiple middle points or *"hops"* - in network-architect terminology. At each of these hops (which are likely to be more then 5) your data can be scooped, copied and potentially modified.

- Your wireless network (your data can be sniffed from the air)
- Your ISP (in most countries they are obliged to keep detailed logs of user activity)
- Internet Exchange Point (IXP) somewhere on another continent (usually more secure then any other *hop*)
- ISP of the hosting company that hosts the site (is probably keeping logs)
- Internal network to which the server is connected
- And multiple hops between...

Any person with physical access to the computers or the networks which are on the way from you to the remote server, intentionally or not, can collect and reveal the data that's passing from you to the remote server and back. This is especially true for so called 'last mile' situations - the few last leaps that an internet connection makes to reach a user. That includes domestic and public wireless or wired networks, telephone and mobile networks, networks in libraries, homes, schools, hotels. Your ISP can not be considered a safe, or 'data-neutral' instance either - in many countries state agencies do not even require a warrant to access your data, and there is always the risk of intrusion by paid attackers working for a deep-pocketed adversaries.

VPN - a Virtual Private Network - is a solution for this 'last-mile' leakage. VPN is a technology that allows the creaton of a virtual network on top of an existing infrastructure. Such a VPN network operates using the same protocols and standards as the underlying physical network. Programs and OS use it transparently, as if it was a separate network connection, yet its topology or the way how network nodes (you, the VPN server and, potentially, other

members of services available on VPN) are interconnected in relation to the physical space is entirely redefined.

Imagine that instead of having to trust your data to every single middle-man (your local network, ISP, the state) you have a choice to pass it via a server of a VPN provider whom you trust (after a recommendation or research) from which your data will start its journey to the remote location. VPN allows you to recreate your local and geo-political context all together - from the moment your data leaves your computer and gets into the VPN network it is fully secured with TSL/SSL type encryption. And as such it will appear as pure random noise to any node who might be spying after you. It is as if your data was traveling inside a titanium-alloy pipe, unbreakable on all the way from your laptop to the VPN server. Of course one could argue that eventually when your data is outside the safe harbour of VPN it becomes just as vulnerable as it was - but this is only partially true. Once your data exits the VPN server it is far away from you - way beyond the reach of some creeps sniffing on the local wireless network, your venal ISP, or a local government obsessed with anti-terrorism laws. A serious VPN provider would have their servers installed at a high-security Internet exchange location, rendering any physical human access, tapping or logging a difficult task.

> *"Today everything you do on the Internet is monitored and we want to change that. With our fast VPN service you get totally anonymous on the Internet. It's also possible to surf censored web sites, that your school, ISP, work or country are blocking. [DarkVPN] will not only help people to surf anonymously, it also helps people in countries like China to be able to surf censored web pages. Which is your democratic right. DarknetVPN gives all VPN users an anonymous IP address. All electronic tracks will end up with us. We do not save any log files in order to achieve maximum anonymity. With us you always surfing anonymously, secure and encrypted."* (http://www.darknetvpn.com/about.php)

Another interesting and often underrated features of VPN is encoded in its name - besides being **V**irtual and **P**rivate it is also a **N**etwork. VPN allows one not only to connect via the VPN server to the rest of the world but also to communicate to other members of the same VPN network without ever having to leave the safety of encrypted space. Through this functionality Virtual

Private Network becomes something like a *DarkNet* (in a broader sense of the definition) - a network isolated from the Internet and inaccessible to "others". Since a connection to VPN server and thus the private network it facilitates, require a key or a *certificate*, only "invited" users are allowed. There is no chance that Internet stranger would gain access to what's on a VPN without enrolling as a user or stealing someones keys. While not referred to as such, any corporate *Intranet* type of network is a DarkNet too.

"A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible.."
(http://en.wikipedia.org/wiki/Virtual_private_network)

Many commercial VPN providers stress the *anonymity* that their service provides. Quoting Ipredator.org page (a VPN service started by the people behind The Pirate Bay project): *"You'll exchange the IP address you get from your ISP for an anonymous IP address. You get a safe/encrypted connection between your computer and the Internet"*. Indeed, when you access the Internet via a VPN connection it does appear as if the connection is originating from the IP address of IPredator servers.

"You'll exchange the IP address you get from your ISP for an anonymous IP address. You get a safe/encrypted connection between your computer and the Internet."
(https://www.ipredator.se)

None of their claims are verifiable! There have been multiple instances of them being caught lying.

They also routinely misuse their chosen VPN tech in ways that negate any usefulness.

USE TOR!

Unless of course you are techeically competent enough to properly run your own tunnel to a leased machine. This provides no anonymity but can bypass "last mile" surveillance in some, if not most, cases!