PRIVACY WAR

Evening the score in the battle for Privacy!

This eBook is brought to you by:

www.PrivacyWar.org
Disclaimer & Copyright..

This information is provided "as is". The author, publishers and marketers of this information disclaim any loss or liability, either directly or indirectly as a consequence of applying the information presented herein, or in regard to the use and application of said information.

No guarantee is given, either expressed or implied, in regard to the merchantability, accuracy, or acceptability of the information. Further, this information is for educational and informational purposes only. The content is not intended as professional advice. Any information found in this e-book, should not be used in a professional decision making process.

Copyright 2012 - www.PrivacyWar.org, All Rights Reserved. No part of this publication may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.
# Table of Contents

- 'Dumpster Diving' ..4
- 'Phishing' Attacks ..8
- Are YOU being tracked? ..15
- CCTV Big Brother Issue ..21
- Online 'Profile Stripping' ..26
- Is the Government SPYING on you? ..32
- Targeted Advertising ..37
- Google - Infringing on your Privacy? ..40
- Putting it all together.. ..47
'Dumpster Diving' ...

How Identity Theft and waste go hand in hand!

In 2011 the estimated total cost of identity theft in the USA was $1.52 billion. This staggering sum of money went to waste because public awareness of the risks of identity theft (and the proper way to avoid becoming a victim of it) is still not at a sufficient level. Many identity thefts this year will be successful as a result of 'dumpster diving' (or 'trash mining'), a technique which, whilst brazen, can be highly lucrative for the intrepid identity thief! The vast majority of people think nothing of throwing mail correspondence away once it has served its purpose. In the case of the humble utility bill, it can even feel quite cathartic to toss them into recycling, safe in the knowledge that your finances are secure for another month.
Once they're in the recycling bin of course, they sit outside the house until they're picked up by a disposal truck. Usually in an unlocked, waterproof container which is instantly accessible to passing strangers- or to a dedicated identity thief. He (or she) will be only too glad to relieve you of your waste paper! Why you may wonder?

Well those seemingly-insignificant pieces of paper that most of us dispose of so carelessly actually contain heaps of critical information about your identity- your name (and those of your family), address, bank account details and details of your insurance policies are listed openly on many official documents. Unfortunately, these are the exact bits of information that are required in order for someone to falsely adopt your identity and cause mayhem.

One man's trash...

You might think it unlikely that, out of all the recycling bins on your street, an identity thief will know that yours contains the things that he/she is looking for. It does sound far-fetched that any sane person is ready and willing to rifle through someone else's waste, admittedly, but this complacency is the very reason that people wind up falling victim to identity theft in the first place!

Ask yourself “do I want to play the odds? Is it worth the risk?”

One of the most common methods employed by dumpster-diving thieves
revolves around credit cards. Many of us receive offers to be approved for a credit card by post—normally cards with a disproportionately high level of APR—which we then throw away. It’s incredibly easy at this point for an enterprising individual to respond to the offer in your name, providing a new postal address to the credit card company. In no time at all (providing your credit score is reasonable) this individual could have a credit card in your name, with which they can run up significant debts without your knowledge. Often the victims will be unaware of what’s happened until they get a phone-call from a lender asking for repayment!

A more public dumpster, such as those outside hospitals or office buildings, are also a fruitful target. In recent years, data protection legislation has dictated that personal information must be stored more securely than in the past and disposed of properly, but medical records especially are desirable for the identity thief as they can provide an extra form of proof of identity when applying for credit.

This method of data collection is very lucrative. Authorities estimate that in the United Kingdom alone last year, identity fraud took place to the value of £1.7 billion. It’s unclear how much of this is a result of dumpster-diving and how much is a result of online identity theft and phone scams, but evidently all of these methods represent an immediate potential danger to us all. Rectifying the damage caused by an identity theft is no laughing matter either— in some cases the victims of this crime only find out they’ve been targeted after a warrant is issued for their arrest. Around 48% of people discover the fraudulent activity within
three months, but up to 18% may not find out for a period of four years or more. Even then, it's estimated that the average victim will spend around 330 hours trying to undo the damage identity theft causes.

How to protect yourself ...

You do have the means to protect your identity!

In spite of the obvious seriousness of this crime, dumpster-diving can be fought against and is preventable, IF you are careful and vigilant!

1) Keep a shredder somewhere in your house (or failing that, a metal bin that's safe for burning things in). Be sure to use your shredder/burning bin to properly dispose of all documents that contain critical personal information, such as bank statements, credit card documentation, gas, water or electricity bills and letters from debt collectors. Cross-cut shredders are ideally suited for this purpose because they cut cards and documents from top-to-bottom as well as left-to-right, providing an extra level of security for items that might be easily pieced together after going through a regular shredder.

2) Take special care with any post that contains your bank account details- if you're going to keep it, make sure it's all in one place and stored away securely. It might be worth investing in a small safe (they can be purchased fairly cheaply, and you can use it to store any other
valuables that could be desirable to thieves).

3) Keep your bins in a location where you or a neighbor can keep an eye on them from the house. That way, anyone who wants to go rifling through your waste will have to do so in full view of the street, which just might be enough of a deterrent to make the potential thief go elsewhere.

3) Old debit and credit cards should be cut up thoroughly (or shredded, if you have a shredder that’s up to the task) so that the information on the card is no longer legible. There is a misconception that because expired cards can no longer be used to make purchases and withdrawals directly, it's safe to simply throw them away. Remember, these cards still carry information about your identity and bank account, and should be afforded as much care as your other high-risk waste!

'Phishing Attacks' …

The Internet is the new Privacy theater of WAR!!

The aim of this book, as we’ve discussed, is to help you to protect yourself from the invasion of your privacy- and at no point is your privacy more at risk than when you’re using the internet. Thanks to the security offered by websites such as Paypal, and the “verified by Visa” service (which allows you to password-protect the use of your cards
online) shopping online is now much safer than it ever has been. However, there is another equally serious threat to your online security that you might be less conscious of: phishing attacks.

‘Phishing’ for a big catch…just not the way you’d think!

“Phishing attacks” are attempts by an individual or organization to fraudulently obtain personal information such as e-mail addresses, passwords, user-names and credit card information. This information is later used to purchase goods or apply for credit in the victim’s name. Very often, the attack will take the form of an e-mail; an e-mail which, on initial inspection, will appear to be from an official organization such as a bank or the tax office.
Typically the e-mail contains a message about fraudulent activity on your account, or instead about cash that you're owed as a result of an overpayment, but there is a fair amount of variation. They do share a common goal though: they want to make you curious. Curious enough, at least, to click the link contained within the message. Below is a genuine example of a typical phishing attack:

This message appeared in my inbox around a week ago. On the surface, it looks like a genuine message from Santander, which is one of the world's largest banks. It has an official looking “Santander” header, and the sender's address is listed as donotreply@santander.co.uk. All very official so far isn't it?

Dear Santander Bank Customer,

YOUR ACCOUNT HAS BEEN FLAGGED AS ONE OF THE NUMEROUS ACCOUNTS THAT NEEDS TO BE REVIEWED.
The main reason for this action are:

* Billing / Payment Issues.
* Invalid log on attempts by a suspected third party user.

We recently upgraded our Online Service to provide a good services for all our Internet Banking Users in order not to experience any difficulties when signing to your internet account.

[Click Here To Proceed]

Fraud Prevention Unit
Customer Service
Santander Bank.

The problem is that I am not, and never have been, a customer of Santander bank! It's impossible that there have ever been any unusual

Copyright © 2012 - www.PrivacyWar.org
activities on my account simply because I don't have an account to begin with. And when you look closer, there are plenty of other clues that this message is an attempt at deception rather than the genuine article. For starters, this message was automatically filtered by my e-mail provider's junk filter. Now, sometimes these filters do make mistakes but in general anything that is assigned to the junk folder should be viewed with special caution. Secondly, you'll notice that the message is addressed to “Santander Bank Customer” rather than to my actual name.

My actual bank account provider tends to use my name in all official correspondence and (to be frank) if they didn't I'd want to know why. The fact that whoever sent this message decided against using my name implies that they didn't know it in the first place and thus the message is fraudulent!

Luckily, the link in this message (which ostensibly should take me to the Santander website) has already been reported as a security threat. My browser tells me this if I click the link. If it hadn't already been reported, I would probably be directed to a page that looks a lot like an official Santander website. Invariably, this is where I'd be asked for my personal information (bank details, name and address amongst others) and the attack would be complete. Interestingly, I could have ascertained that this was an attempt at fraud by hovering over the link in the message with my cursor- it directs me to the following URL: “http://www.friendshipgardens.org/wpincludes/images/wlw/forms.asp.htm”
This certainly doesn’t look an awful lot like the official Santander banking website to say the least!

Some estimates suggest that there are as many as 900 unique phishing attacks every day. Each of those unique attacks can be copied and forwarded to hundreds of thousands of in-boxes worldwide- resulting in a total number of phishing attacks each day which exceeds ten million.

This is the real “strength” of the phishing attack as a concept- although it has a very low success rate (most people will notice something is amiss before the attack has reached completion), the sheer number of attempts makes even a low success rate extremely profitable. In the USA, in 2011, an estimated 0.47 percent of bank customers fell victim to some variety of phishing attack, which equates to between $2.4 million and $9.4 million lost for every million online banking customers per year!

'Tabnabbing' ...

A new & emerging form of Phishing Attack on your privacy!

Tabnabbing is a newer type of phishing attack, named by designer and security researcher Aza Raskin in 2010, in reference to the fact that this method of phishing works by taking advantage of any tabs left open on your browser for an extended period of time.
While the user browses other websites, a piece of HTML or Javascript rewrites a tab that has been left open to resemble a well-known site such as Hotmail or Gmail. An internet user who returns to this tab will presume he/she has been logged out of their e-mail inbox after a period of inactivity, and attempt to log back in. Of course, the site they're now entering their details into is a mock-up of the genuine one, and exists only to steal user-name and password information.

Think about how many times you've done just that. Maybe you've left for a few minutes to grab a drink, or speak to a colleague. It is happening everyday to people and it could happen to you too. Pretty scary stuff isn't it?

'Pharming' …

Beware the weapon of choice..BOGUS sites!

Pharming can be considered a derivative of phishing, and works in a very similar fashion. The difference is that instead of directing users to a realistic-looking imitation of a genuine website, this technique works by redirecting an entire website's users from its genuine URL to another, bogus website. This may be a more efficient technique than the average phishing attack, and certainly one that is more difficult to spot. This is because 'pharming' doesn't rely on users clicking on a “bait” link (as we
discussed above) but rather redirects genuine traffic. However, it is more difficult to carry out. Here’s why.

Pharming requires direct access to a user’s computer or a server. The most common way to initiate the attack is by a technique called “DNS poisoning”, which works by manipulating the naming system that allows a user to assign URLs rather than IP addresses to websites in order to make them easier to remember and access later (for example, replacing “192.168.0.2” with “www.email.com”). By changing the way this naming system works, the successful pharming attack can alter the direction of traffic for large sections of the internet.

Anti-spyware programs will generally fail to pick up or prevent a pharming attack because in strictly technical terms nothing is wrong with the affected computer. In order to be properly protected against pharming you must be extremely vigilant whilst browsing the internet - regularly checking the address bar, for example, to make sure that the URL you’ve entered doesn’t change for no reason. Also look out for a padlock or key symbol along the bottom of your browser task-bar.

A locked padlock or a key indicates a secure connection, whereas an unlocked padlock or a broken key indicates that your current connection is insecure - close that page down right now if you’re entering financial details!
How to protect yourself ...

Prevent Phishing from getting its hook in to you!

In order to effectively stay safe from all types of phishing attacks you can employ a set of tactics designed to throw the phishing attempt off your track. Be sure to take the following steps:

1) Carefully inspect any e-mails that wind up in your “junk” folder. Nine times out of ten they will have been assigned to this folder for a reason after being reported as spam by other e-mail users.

2) If you're not a customer of the organization that appears to have sent the message, it's generally a good idea to ignore it entirely - especially if the message is to report unusual activity on your non-existent account.

3) Does the e-mail contain your real name? If not, you should question why. Any company that has or wants your custom will probably take the time to learn it before they contact you.

4) REMEMBER, Banks and other finance-based organizations will never ask for your account details via e-mail. If your email is from a bank, and they ask for this information, never give it out. When you hover over the link in the message, does it take you to an official site? Look out for slight, but unusual, variations in the URL that are indicators of a phishing attack.
5) Pay attention to any information your chosen internet browser program gives you. Most browsers are now equipped with anti-phishing software and will often alert you if you try to browse any 'known' phishing domains, so PAY ATTENTION.

Are you being tracked? ...

Is your cellphone giving away your location?

Believe it or not, the ability to track someone’s location using the signal transmitted by their mobile phone is generally seen as the occupation of homicide detectives in the latest Hollywood thriller. Surely, even if this is possible with the use of some super-secret technology, we’re not all traceable via our cellphone signals... are we? It’s a worrying prospect for most of us, at least those of us who value our right to privacy.

The unfortunate truth is that your location CAN be attained, accurately and (almost) instantly by your mobile service provider!

There are several different methods used for this purpose:

**Multilateration..**

Multilateration works by using the signals exchanged by your cellphone and a pair of radio towers to measure the difference in distance
between you and the two towers. Initially this allows a 'hyperbolic curve' to be plotted, which itself contains an infinite number of possible locations where the measurement is correct. Then, a second curve is plotted by the same method, but using a different pair of radio towers. The two curves (from the first and second sets of measurements) will intersect at some point, giving a small number of possible current locations (a “fix”).

**Control Plane Locating..**

Control Plane Locating is a slower and less accurate method, which relies on gauging the radio-delay between a mobile phone and its nearest mast. CPL is used most frequently in European countries, and only as a safety measure because of its low cost and minimal impact on equipment.

**GPS..**

GPS (Global Positioning System) is the most accurate way to attain the location of a mobile phone, but is not always a feasible option because only higher-end mobile phones tend to have the this technology installed. It works by trilateration (a method nearly identical, but more accurate than, multilateration which is mentioned above) and can typically be considered accurate down to a distance of a few meters. GPS is also the only method that works even when the mobile phone is not communicating with cellphone masts!! (more on this below).
So where's the threat to your privacy?
Frighteningly close to home actually..

In 2008, for the first time, the FBI used techniques like those mentioned above to track the location (and previous locations) of a group of armed robbers who had carried out armed raids on as many as 20 banks in Texas, USA.

Not only were they able to ascertain the previous locations of the robbers, they were also able to identify the men themselves- by combing the data logs of cellphone companies in the area of the robberies they discovered that two particular mobile phones had been in use around the time of every robbery. From that point it was a simple case of arresting the owners of the cellphones, who were later charged with multiple counts of bank robbery and firearms offenses.

The legal statutes surrounding this kind of tracking were unclear at the time- having been written an entire generation ago, they didn't account for the latest technologies. The current presidential administration said it believed that American citizens are entitled to “no reasonable expectation of privacy” regarding their locations or that of their mobile phones, and that no rights are being violated when a service provider allows the authorities access to its records. Understandably, these arguments raised the hackles of civil rights groups, who argued that privacy laws need to be updated- taking into account recent advances in mobile hardware.
The supreme court (in a test case that was put together to test whether or not it would be lawful for federal agents to attach a tracking device to someone’s vehicle without their knowledge or consent) eventually granted American citizens new rights to privacy against warrant-less government tracking - but stopped short of clarifying these rights properly - for example, no mention was made regarding when exactly a warrant for tracking would be required!

This ambiguity means that there could well be loopholes in the new privacy rights that allow continued cellphone tracking by government agencies - a fact which still alarms proponents of civil rights!

That’s not the only Privacy worry here..

As we've already discussed, it is entirely possible for a person with the necessary resources to track your position in real-time using measurements taken from the nearest cellphone towers that your phone is communicating with, or more accurately by tracing the GPS chip contained within many of today’s more expensive mobiles. In order to use these methods to locate someone, however, federal agents must first obtain a warrant.

Worryingly though, there is a much newer technique that requires no assistance from mobile service providers whatsoever - a technology that’s code-named “Triggerfish”.

Copyright©2012 - www.PrivacyWar.org
Triggerfish is a surveillance technology that intercepts cellphone signals in order to discover the locations of specific phones! It does so by using a mobile cellular base station (also known as cell-site simulators or digital analyzers) to either:

a) Find the location of a specific cellphone (without a GPS chip) by scanning for its emissions.

Or

b) Mimic an actual cellphone tower, and in doing so, force a specific mobile phone to reveal its phone number, serial number and location.

Or

c) Intercept a phone-call to specific cellphones (whether the call is made or received).

The ‘Triggerfish’ device does, by law, require a court order before it can be used, but circumvents the provisions in the ‘Communications Assistance for Law Enforcement Act’ that forbid the use of pen register or trap-and-trace devices. Clearly this technology presents a real risk, in the wrong hands, to our privacy. So how do we avoid being found when we’d rather keep our location secret? The unfortunate reality is that if you need to use your mobile phone in any capacity, evading location via these methods is all but impossible.
A person, or group of people, with the means and the know-how to do so can discover your location by tracking your cellphone as long as it’s on-regardless of whether or not you’re making a call. Evidently, the only way to remain under the radar is to leave our phones at home-preferably turned off, and with the battery removed.

If you absolutely must have a mobile phone with you at all times, seriously consider using an outdated model. They might not be very fun to use, but few cellphones from six or seven years ago will contain a GPS chip and this might offer you at least a thin layer of protection against unwanted attention. Older phones are also much cheaper, meaning that you can discard and change your mobile phone regularly if you’re especially concerned about surveillance.

A very similar approach to avoidance is by using disposable phones (sometimes called ‘Burners’) to make any necessary calls. These can then be disposed of in the nearest bin and a new one purchased. This technique can work well if you have a real concern for your privacy—Just be sure to ditch the ‘burner’ once you’ve used it once.
The CCTV Big Brother Issue …

Yes, Big Brother certainly is watching. But the real question should be, who else is watching too?! Closed-circuit television, or CCTV is the use of video cameras to monitor a variety of locations at one central site, such as a control room, where the video feeds are displayed on monitors.

These cameras have become particularly prevalent in the USA and UK, where they were introduced during the 1970s and 1980s in trials to test their effectiveness as a deterrent to crime as well as a means of identifying and arresting criminals in the aftermath of an incident. In the UK in 1994 they were deemed successful by a government report, and thus that year saw a massive increase in the number of cameras in use - and the number of cameras has continued to be increased every year since then. Today, almost every city center, fuel station forecourt, vehicle for public transport and retail store is covered by a network of CCTV cameras covering every angle.
The exact number of cameras varies across countries, and then again by states or counties, however as an example, the best estimate is that there are roughly 1.85 million CCTV cameras currently in use throughout the UK, a number which doesn't include smaller systems used by off-licenses that tend to be paid for privately. This translates to roughly one camera to every thirty-two people in Great Britain.

Now consider that the UK is a fraction of the size of the USA and we are talking about phenomenal numbers of CCTV cameras! It is estimated that the average person can expect to be captured by up to 70 different CCTV cameras per day, although many of those will be brief glimpses on the periphery of the shot. In the USA there are an estimated 3.6 million CCTV cameras and in recent years there have been moves to bring the USA “up to speed” in terms of camera numbers in the belief that it will reduce crime rates - contrary to previous US opinion that downplayed CCTV’s value.

But why is my privacy being invaded like this?

The efficacy of CCTV in preventing crime varies widely - studies suggest that crime in parking lots, for example, is cut in half by the presence of CCTV cameras whereas in public settings the cameras only reduced overall crime by 7%. However, the cameras appear to be much more effective at identifying and locating suspects and witnesses in the event of a crime, and anti-terrorist police have routinely made use of CCTV to monitor terror suspects since the 1970s.
More recently, cameras have been installed on public transport in response to increasing anti-social behavior and criminal behavior on the trains and buses. Mobile Police surveillance vans also carry CCTV units that are equipped with number plate recognition technology, which is linked to the DVLA database and helps Police identify cars that are on the road illegally.

The good, the bad and the ugly..

Many people are disconcerted by the massive volume of CCTV cameras they see on a daily basis, and understandably so, as it does seem like an encroachment on our right to privacy. After all, nobody would enjoy having a camera follow them around all day, let alone appearing on up to 70 different cameras daily! Unfortunately though, on most occasions individuals have no right by law to try and prevent these cameras from monitoring their movements and behavior - the owner of the CCTV camera even has the right to archive footage in which you appear.

However, it is illegal for anyone to use that footage to try and obtain information about you personally (with the exception of Police officers and federal authorities).

Introducing… “Internet Eyes”

In 2011 a website called “Internet Eyes” was launched that allowed Internet users to monitor CCTV cameras from their homes, with cash incentives of up to £1000 for anyone who regularly spots and reports...
activity such as shoplifting in stores - with the relatively obvious aim of deterring crime and anti-social behavior and apprehending those who commit crime without further stretching Police resources.

Subscribers are given four cameras to monitor at a time and are instructed to hit an “alert” button if anything out of the ordinary takes place. This immediately notifies the store manager by text and picture messaging, who can then decide on the correct course of action to take. However when the site was launched publicly, it was harshly criticized.

Civil liberties campaigners in particular felt it represented a “distasteful” approach and was encouraging citizens to spy on one another. Their fears were somewhat vindicated when footage from the site began to appear on video-streaming site YouTube, prompting an investigation which led to significant changes to Internet Eyes’ operating policies.

For safety purposes, subscribers were not allowed to view images from cameras within a 30-mile radius of their home. Also, due to privacy infringement concerns, the video feeds are now encrypted to prevent any recordings appearing on YouTube in the future - so it looks like the concerns that were raised last year have been dealt with.

However, there does seem to be an increasing tendency towards using CCTV for things other than its original intended use. Recently there have been incidents in the UK of local councils using unmarked CCTV cameras
to record trivial traffic offenses and hand out fines, and for many this trend is putting a slightly 'Orwellian' spin on the situation. The use of CCTV is governed by the Data Protection Act in the UK and similar legal frameworks in other countries, but unfortunately in many cases its use is subject to guidelines rather than law and as such the owners of CCTV units have a fairly free-reign as far as their use is concerned.

For now though, most polls indicate that the general public supports rather than opposes the proliferation of cameras in their local area. Admittedly it has been put to excellent use in high-profile cases such as the 7/7 attacks in London and the murder of James Bulger in 1993, and in that respect it is a fantastic tool for the justice system. Let's hope the public's right to privacy continues to be paramount elsewhere.

How to protect yourself ...

Keeping away from prying eyes...thousands of them!

As we've just discussed, there's a very murky cloud around the issue of privacy infringement due to the use (or misuse) of Closed Circuit Television (CCTV) recordings, one which blurs boundaries on a regular basis. It's clear to see that civil rights campaigners and those who are simply trying to protect their rights to privacy do have a very valid reason to be concerned.
However due to the CCTV issue being an integrated part of the infrastructures of the towns and cities where we live (such as being built into the construction of shopping malls or government buildings) there are a limited number of steps we can take to avoid this.

1) Your reason for wanting to stay out of the view Big Brother’s eyes are your own, however head-wear such as peak caps or brim hats are a great way to avoid the camera, as most cameras are positioned on elevated angles.

2) Sunglasses or ‘shades’ are intentional and effective ways of making identifying you more difficult as dark sunglasses can hide facial features when caught on CCTV other than just eyes.

3) The most obvious tactic to avoid CCTV cameras is to be aware of their location and vary your journeys. Alternatively avoiding areas which are undoubtedly covered by camera angles is the most foolproof way however inconvenient. Do remember that vehicle plate recognition software exists in many cities for “public safety” and law enforcement. So even though you may avoid being caught on camera personally, it’s always worth remembering that public transport (although heavily CCTV covered) is a better means of avoiding identifying yourself in a link with a particular vehicle.
Online Profile Stripping ...

The most vulnerable aspect of social media!

Profile stripping is perhaps the least well-publicized threat to your identity, but because it’s so straightforward to perform it may well pose the highest risk to your personal privacy!

Profile stripping has emerged as an identity theft and identity exploitation technique drawn from the opportunities provided by the popularity of social networking and media websites such as Facebook, Myspace, Bebo and Twitter. These sites are promoted as a way to communicate with friends (and make new ones) quickly and easily, as well as a way to share media such as music and photographs freely.

They encourage users to participate by listing their preferences and joining groups based on where they work and live. After just a short period of time, a site such as Facebook holds an incredibly detailed picture of your life, past and future. The photographs you upload show people what you look like, and you’ve probably posted plenty of clues as to where you live and work, as well as who your family are and what you enjoy doing.

Don’t underestimate the risks of social websites.

None of this information appears to hold any special significance, and you could be forgiven for thinking that it poses any risks to you, even in
the wrong hands. Sound about right?

Sadly, you'd be very wrong. This method is sort of a hi-tech equivalent the the dumpster diving technique we've already mentioned earlier in the book. Except, instead of climbing into a dumpster and hoping for the best, these online identity thieves look to compromise the security of social media sites because they know for a fact that there are millions of people's personal information inside. And keeping our information secure is no easy task for the owners and of these websites!

The intangible nature of data stored on the internet makes it impossible to simply put a heavy-duty padlock on something and call it a day. The people looking to access these crucial bits of data are often well-versed in computer “hacking” techniques and advanced programming.

Consequently none of your personal details, once saved onto a site such as Facebook, can be considered secure. Luckily this doesn't mean that we can't all stay safe online, as long as we're frugal with the information we submit to online forms. Remember, all of the information that social-networking sites hold is information that you've given them willingly, so it's best not to be too forthcoming with the following pieces of information:

- Details from your passport
- Driving license
- Bank or credit cards (Unless into a secure form)
• Home address/es
• Your current or previous employer
• Your full name
• Real date of birth:

There's no good reason to include your middle name when using social networking, and it can't hurt to alter the year on the date of birth field either. Both of these pieces of information can be very valuable to anyone looking to 'strip' your profile.

Who are you really speaking to??

When using the internet, it's impossible for you to be sure that you're talking to the person you think you're talking to. Most of us would be extremely wary if a stranger added us as a friend on a social networking site and immediately began asking questions, but what if someone we've known for years asks the same questions? You'd more than likely answer without a second thought, right?

The answer is that you should always tread carefully when you're answering questions about yourself. If someone manages to gain access to a friend's account, they will almost certainly speak to their immediate friends to fill in the blanks for any info they're missing or to try to access further accounts (namely yours). This is simply like completing a giant jigsaw puzzle!
In order to get access to your profile, an individual will need your password. It is essential that you choose a secure password that can’t be guessed at by someone who knows your name, your pet’s names or your children’s names etc. The top 5 most commonly used passwords of all time are as follows:

1) 123456
2) 12345
3) 123456789
4) Password
5) iloveyou

As you can see, three of those passwords are a simple set of numbers in ascending order and another is the word “password”. None of these should be considered secure on any level. Ideally you should pick a password that includes both letters and numbers, preferably without any dates or names that could be taken from information you’ve posted online.

When setting up an account, many sites have an indicator of password strength to help you gauge the quality of your current password- the higher the strength of your password, the less likely it is that anyone will be able to guess it.

Don’t use anything that can be seen or drawn from your profile!
If your password is too difficult to guess, a dedicated thief might also attempt to guess the answer to your security question - which exists to allow users to access their accounts in the event that they forget their password. Often there is a choice of several possible questions such as “What is your mother’s maiden name?” and “What’s the name of the street you grew up on?”. Again, if you’re going to give an honest answer to these questions it’s essential you choose one that can’t be answered by someone other than yourself.

How to protect yourself …

The keys to locking up your profiles!

So now you know the risks, you need to know the techniques to protect your valuable information and privacy proof your online accounts.

1) Make sure that everyone in your family that uses a computer is aware of the dangers of ‘profile stripping’. Remember that the elderly, and especially children, are more likely to be naive regarding potential threats to their identities but are still at risk of becoming victims. If your children are under the age of 16, it might be worth checking their profile pages on social networking sites once a week to ensure that nothing suspicious is taking place there. If they’re especially young, you may even consider blocking access to social networking sites from your home computer. ID fraud aside, these sites can be dangerous to young,
vulnerable users for a host of reasons.

2) As discussed, many passwords are either made up of the 5 common choices listed above, or can be found within the information on one of your social networking sites. Seemingly harmless information can often prove to be the way in for profile strippers.

3) Consider using alternative details on your profile. For instance choose a date of birth that indicates your correct age but does not disclose your exact date of birth, this way if it is used to attempt to gain access to other accounts - financial/personal or social - it will fail.

Is Your Government Spying

...On You?

So you're not that interesting? Think again..

In the aftermath of the tragic terror attacks on the 11th of September 2001, in which nearly 3,000 people were killed, the suspicion in much of the Western world was palpable. In many countries, the subsequent uncovering of so many terrorist plots in the USA and Europe led to new legislations regarding privacy, surveillance and the detainment of terror suspects. In America this legislation took shape in the form of the USA PATRIOT (an acronym that stands for Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and)
Obstruct Terrorism) Act that was signed into law by George W Bush on October 26, 2001.

The act represented a fairly drastic reduction in the day-to-day freedoms of the American public, as well as an increase in the freedoms granted to law enforcement agents with regards to the gathering of intelligence. It also gave the Secretary of the Treasury more authority to regulate financial transactions that involve individuals of a non-American nationality, and changed the rules regarding the detention and deportation of immigrants suspected of terrorist acts and the definition of “domestic terrorism”.

Controversy has surrounded the act since it was passed in 2001. PATRIOT was passed by both houses of congress as little as 48 hours after its final wording was complete. Allegedly, few or zero US senators actually read the act before passing it, which is remarkable in itself given the magnitude of the provisions it contained. Critics said that an act with
such far-reaching repercussions warranted much further deliberation than it was given, and suggested it was rushed through congress in order to take advantage of its close proximity to the 9/11 attacks.

Some of the act's provisions have been called unconstitutional, as they appear to severely impinge on some civil liberties such as the right to privacy - which is not implicitly mentioned in the constitution but has frequently been supported by the Supreme Court. This right to privacy has been compromised by expansion of the ability of the government to set wire-taps and carry-out searches without prior notification.

There is also some concern that the provisions of the PATRIOT act might be exploited for use in non-terror related crime, and there are questions being raised about how exactly information is being used. For example, reports suggest that it has already been used incorrectly to collect financial data about tourists in Las Vegas.

The highly publicized nature of the USA PATRIOT act and its criticisms has put the American public in a very uncomfortable position. This legislation was put in place ostensibly to aid the war against the terrorist groups that have done so much harm to the country over the last decade, so (and this is convenient for supporters of the act) to criticize it can seem- for want of a better word- unpatriotic. However, with growing concern over misuse of the government's new surveillance capabilities, how do you know you're not being watched by your own country?
Being watched in MY OWN country?

Details of any specific or intentional incidences of activity that involve US agencies and misuse of PATRIOT provisions are unclear. Those ‘in the know’ are forbidden from releasing specifics due to their obligations to secrecy under law. The worry seems to be that ordinary, law-abiding citizens’ communications data (such as e-mails and phone records, amongst other things) may be inadvertently gathered by intelligence services when they cast their nets for terror suspects. There is a suggestion that this information, however innocently it’s acquired, may be cataloged for future reference and even used as evidence against people for whom there has been no search warrant issued.

Calls for information on just how many people in the United States have had their communications reviewed (as part of investigations under this act) have so far gone partially unanswered. The National Intelligence Agency has so far said it would not be feasible, or even possible to identify every person whose information they’ve reviewed.

Another very real concern exists around government ability (and willingness) to track the location of its citizens via the GPS chips in their mobile phones (as we mentioned earlier in the book). Quotes from a senate hearing on the subject suggest that there are circumstances where permission to do so could be granted to the authorities.

Ultimately, it seems unlikely that the US government is spying on you personally, or rather intentionally. This might not be the comforting
news that it appears to be at first glance, though. The available evidence suggests that your information might be collected collaterally, albeit without explicit intent, and stored for future reference. This is a dangerous step towards an attitude of presumed future guilt and the use of national security as an excuse for infringement on constitutional rights.

The NSA Spying Facility..

At some point in 2013, the NSA will complete the construction of the $2 billion “Utah Data Center”. The vast, 240 acre site will house (amongst many other things, undoubtedly) numerous servers and databases dedicated to sifting colossal amounts of data- including the contents of e-mails, phone calls and Google searches performed by American citizens- into a single, gigantic database. Eventually every user of a cellphone or computer in the USA will be profiled on this database- someone, somewhere will have access to details of your recent purchases, travel receipts and internet history.

Of course, the fact that authorities are collecting this information is far from breaking news. As early as 2006 (and very possibly before then) the NSA were revealed to have set up special monitoring rooms in the major US telecoms facilities for this exact purpose- as many as twenty of them, according to some sources. The open centralization of this subterfuge to the UDC seems to suggest that their efforts are being turned up a notch, and in the face of global financial difficulties you have to wonder if there aren’t better uses for $2 billion!
The fun doesn’t stop there, either. The facility will also serve as a center for breaking codes, specifically encryption on financial transactions, exchanges between foreign ministers and dignitaries, and personal communications too. How important will your privacy be when there is literally no way for you to enforce it? The necessity of these invasions of privacy will be argued in terms of counter-terrorism and national security, and undeniably the ability to intercept and decode messages at will is crucial in combating any threats therein, but giving intelligence services a proverbial blank check to do as they please seems like a dangerous step towards the potential totalitarian state that is of such grave concern to so many people.

**How to protect yourself ...**

*Adopting a routine to protect yourself!*

As technology advances at frighteningly quick rates, the available methods and techniques used by the government are increasing too. While this appears to be a blow in the battle to retain your privacy, there are ways open to us which can help provide a barrier between your life and those bent on infringing on your privacy.

1) One of the most effective and seemingly obvious approaches is to carefully consider how you share your sensitive information with others. This applies to everybody you interact with, from family and colleagues to friends and partners! Now you are aware of the vulnerabilities that
the digital and online world have, do you really think it's safe to send private information over these mediums? No, of course not. Replace email and text messaging with old fashioned hand written letters or better still, face to face conversations. Why? Well essentially, apart from on rare occasions, these methods of communication are not recorded. This means nobody can retrieve a record of what was said at a later date.

2) A similar approach and similar considerations should be given to using the telephone or your cellphone. Do not pass any important or sensitive information during these conversations. If you absolutely must, try and be selective about the extent of the details you pass.

Targeted Advertising..

Even your buying habits are being exploited!

Have you ever wondered why the advertisements on sites such as Facebook always seem oddly suited to your interests? If you've been visiting a lot of health and fitness related sites recently, for example, you'll probably be shown some ads for the latest piece of gym equipment or health supplement. Or if you shop online for clothes quite often you might be shown ads for a new online clothing store. This is called “targeted advertising”, and on the surface it seems like a pretty good idea. After all, there's no use advertising women's footwear to male
customers, just as there’s no point in advertising men’s hair products to women.

It's the methods used to acquire the info that's questionable.

A “cookie” is a set of data that assists internet users in connecting to websites, or storing preferences to make future connection to sites you've visited quicker. They are generally stored by your computer without your knowledge or express consent, and the cookies on your computer provide in-depth information about the sites you've visited and your general behavior patterns online.

For this reason, they are incredibly valuable to advertisers who want to tailor their ads to each individual user. In 2009 it was also discovered that cookies could be linked to social networking profiles- which is how you receive your targeted advertising today. In itself, this doesn’t represent a particular severe invasion of privacy, because your cookies can be deleted manually via your browser. Many internet users do this on a set basis anyway. However, online advertisers have refused to draw the line at using cookies to gather information- specifically because they can be deleted.

A substitute, called a “Persistent Identification Element” or “PIE” exists, which is similar to a cookie but holds a significantly higher amount of data and, crucially as it's a Flash cookie rather than a HTML cookie, is much more difficult for a user to delete. This forceful approach to gathering personal information is less in keeping with privacy laws and
It's one thing to monitor people's habits when they're aware of the observation and able to put a stop to it, but developing methods that take away the user's ability to maintain privacy online has an air of "spying" about it.

PIEs, aren't the worst software tool for targeted advertising. That award goes to a javascript application called the "evercookie". Like the regular cookie, it collects user data from the computer on which it's present for marketing and advertising purposes (amongst other things). The difference is that an evercookie persistently creates copies of any cookies it creates that the user attempts to delete.

In short, an evercookie will not allow itself to be deleted. This means that regardless of consent (or express lack thereof) a user with evercookies on their computer can have their internet usage monitored by a third party.

How to protect yourself ...

Keep is simple, keep it clean!

Virtually every single one of us who regularly use the Internet will access it through a well known browser. Primarily this will be Google Chrome, Internet Explorer or Mozilla Firefox. These days all major browsers have options somewhere in the preferences which will allow you to disable cookies on your PC or laptop. This protects against unwanted HTML and
Flash cookies, but can hinder the functionality of many websites severely.

There is an add-on for Mozilla Firefox that allows you to avoid picking up evercookies, ironically called “Nevercookies”. Nevercookies works by extending the built-in private browsing mode on Firefox to protect from evercookies continuously. This is an option seriously worth considering, as larger websites such as Hulu and Spotify are already using this technology and others won’t be far behind.

As a secondary tool for your privacy toolbox you should always develop a regular PC ‘maintenance’ routine. Again most browsers will allow you to do this in a single process but make sure you delete all browsing history, cookies and unused favorites. Be careful if you use the auto-fill option for web forms which is installed on Chrome, Firefox and IE.

Don’t forget that anybody using your computer will see your form filling details appear when they begin to type into an online form! By removing cookies, histories and preferences you’ll keep your computer as sterile as possible. It’s also worth noting that many browsers also offer a private browsing mode whereby no details are kept or stored of the online session!
Google - Infringing on Privacy?

The global giant isn’t as friendly as you might think!

Google is one of the biggest, if not the biggest global names both online and offline. Granted, they offer many amazing features and services that have left people in awe, however, have we really stopped to consider the price we’re unknowingly paying? After all, nothing in life comes free.

Recently, there’s been a lot of buzz about Google and it’s associated privacy infringement. Once upon a time, Google was just a simple search engine. You could type in what you were looking for and get your search results. Nowadays though, Google seems to have taken over the Internet and has undoubtedly monopolized the online world.
One of the biggest and most controversial issues that people have dealing with Google is the fact that it is nearly impossible for anybody to be anywhere without being able to be traced. There has been much scrutiny for Google’s practice of using the Street View application in order to gather information on the locations of millions of cell phones, lap tops and other Wi-Fi devices.

This is being done all over the world and is supposedly done with the purpose of data collection for Street View, which is a hugely popular Google map service. The debate over whether or not this should be allowed rages on as Google effectively ‘spies’ on the users of ‘smart’ devices. Using the phrase ‘Spy’ may seem a little strong, but if there is really any doubt about its validity, the reader should type in their address to Google Street View and prepare to be shocked when they see a crisp and clear picture of their home. Not a huge deal to you? Perhaps not everybody would be concerned with an image of their home appearing online. However how about if we consider that in some circumstances vehicle make, model and even registration plates can be seen too.

Remember how we discussed online ‘profile stripping’ and described it as a jigsaw of information? Each piece leads to another until eventually there’s enough available to do some damage through identity fraud, identity theft or plain and simple financial theft.
We started with a Street View image of a house, then parked a car on the drive. Then associated a vehicle index with the car. Now we have an address, vehicle and registration all linked to one another thanks to Google. If I was to ‘dumpster dive’ at this address I could probably find the name of the occupants. Next I’m on to Facebook to see if that person has listed personal information such as date of birth or place of birth. I now have Name, Address, Date of Birth, Car details, maybe place of work and family details too.

More than enough information to commit identity theft!

Another Google program that has raised major concerns is Desktop. This has recently opened up a lot of privacy issue questions. The most significant concern is that one can share and search information from multiple devices by using only one account. Basically what this means is that one user could use one desktop computer account to search and index, allowing them to file share between several different computers.

Google argues there it is debatable as to whether or not a valid privacy concern exists here, however the one feature that sets off big red flags is the update that gives the user a certain amount of ability to index files and store them on the Google’s servers temporarily.

Without reading the fine print (and many users do not do this) this update gives Google the right to have access to your stored files for thirty days and there is no way to get around this “rule”. Allowing a
major corporation the rights to your intellectual property is a risky game to play, especially when you have given this permission unknowingly.

**Private messaging.. but how private is it?**

Many people use instant messaging and of course Google has their own program available - Google Talk. Again, many people simply click “agree” when it comes to setting up your account and agreeing with their privacy policy. Should you actually read the policy, you might never actually click the ‘agree’ button! The privacy policy is so long and convoluted that it's simply too difficult for the average person to fathom. Just one small part of the agreement states that:

“You agree that Google may access or disclose your personal information, including the content of your communications, if Google is required to do so in order to comply with any valid legal process or governmental request (such as a search warrant, subpoena, statute, or court order), or as otherwise provided in these Terms of Use and the Google Talk Privacy Policy. Personal information collected by Google may be stored and processed in the United States or any other country in which Google Inc. or its agents maintain facilities. By using Google Talk, you consent to any such transfer of information outside of your country.”

Think of it like this: a company as large as Google has so much information going through it each day that nothing ever gets deleted. One must ask themselves how important it is to keep their private
correspondence private before agreeing to the terms of service? The same thing applies when using Gmail accounts and the Google Tool Bar! The tool bar may be a convenient time saver but it also allows this mammoth corporation to track and store every site that you visit and every search you perform. The bad news is that there is not much that can be done to stop them from trying to pry into your private lives short of filing lawsuits that are tied up in litigation for years on end. The good news is that there are some steps that can be taken in order to throw them off your scent and protect your privacy just a bit more.

How to protect yourself …

Building your defenses against the Google Giant!

1) To address the issue of preventing Google from monitoring your toolbar usage, you can use a technique called 'Host File Modification'. This will throw them off and prevent them from being able to track everything you do from their tool bar. This can be a bit complicated, but to find out exactly how to go about performing this task you can go to: http://www.howtogeek.com/howto/27350/beginner-geek-how-to-edit-your-hosts-file/.

This site will give you clear and concise instructions on how to do this.
2) If you aren't particularly concerned about this privacy aspect, you can simply use a search proxy, such as scroogle.org, when doing any sensitive search activity.

3) Ensure you always log out of your Google account while performing searches or visiting sites you'd rather not have recorded. Whilst not entirely foolproof, it provides another layer of protection for your online activities.

4) Another option which will allow you to use the Google services without being virtually tracked is to open a new account under a false name. While this can throw Google off as to whom you really are, it does not stop them from following your activities. However, if you simply wish to have an internet experience without feeling as if you are personally spied on, this is a viable option.

5) Since Google is now also monitoring additional services which are Google owned (such as YouTube and Picasa) and you can't get around logging in to use these services, a clever approach is to use different browsers for each task, which separates your identity. You can install multiple browsers on your computer operating system easily and quickly.

6) There are various services available that can take your identity and mask it from Google. These often require a download (and usage may slow down your surfing) but in doing so you'll employ a tactic of making your email retrieval systems and search results go bouncing around through several servers to even get to Google.
This can really confuse Google and protect your privacy. A service such as this is referred to as an **Anonymizer**.

For superman privacy, do some research on your browser and find its privacy mode section. Some are more obvious than others but almost every one will have this facility. Here you can go into stealth mode so that nothing you do is able to be recorded in your history, and any files that are added by the sites you visit will not be tracked.

While all of these things will help you to protect your privacy from the prying eyes of the Google giant, nothing is truly fool proof except for staying offline. The only real way that affords you 100% privacy is to disconnect from the World Wide Web. This is not an option for most of the western world so try out the above tactics and keep your private life private.

**Whatever you do, say or post online is there forever!**

Keep this in mind and the chances are low that something will be able to come back and bite you later. These days, social networking sites are used more and more frequently in the recruitment sector, both by companies internally and recruitment consultancies. It’s easy to disguise a ‘colorful’ past in an application form but no matter how hard you try, your social networking accounts will always give a truer, clearer picture of the types of things you do and the sorts of people you associate with!
Putting it all together..

It’s time to stop reading and start doing!

Over the past chapters of this book we’ve discussed in depth the serious risks to your privacy which we face in our everyday life. We’ve talked about the methods employed by both individuals seeking to extract and exploit information from you to be used in criminal activity such as financial fraud and also by corporations who look to spy on your behaviors and patterns in an attempt to make commercially sound decisions based on watching you.

Each chapter not only discussed the details of these threats, but also the drivers behind each method! We’ve then provided you with a series of steps and tactics that you can build into your arsenal designed to provide you with layer upon layer of personal privacy security! As a result of a better understanding, you should be more able and better suited to fight back in the war on privacy infringements and exploitation!

There may however, be times when these methods are defeated, or are simply not in place quick enough! The next best thing to prevention is early detection. If you can catch an infringement quick enough, you may be able to limit the damage caused and restore the security of your details faster. We’re primarily talking here about financial breaches of privacy and identity theft, which can have a staggering effect on your life!
Pay close attention to when you receive statements or bills from your bank and your creditors. A missing statement may be a warning sign; identity thieves who gain access to your bank or credit card account often change the billing address to hide their activity. A missing statement may also be a sign that the document itself has been stolen and could be used to gain access to your account!

Contact your bank or creditor immediately if you notice anything!

When you receive bills or statements, read them carefully. Look for charges for things you did not buy or services you did not use, or changes in the personal information listed on your statement. This may be a warning sign that an identity thief is using your account or credit card. One of the best things you can do to assure yourself that your identity is safe is a thorough review of your credit report. Look for debts that are not yours, which may indicate that an identity thief has taken out a loan or a credit card in your name.

You should also pay careful attention to the personal information in your credit report, such as addresses, job history, and other data; if you see an address or employer you do not recognize, this could be a warning sign that someone else is using your name or your Social Security number fraudulently.

Obtaining your credit report is actually pretty easy. The ‘Fair Credit Reporting Act’ requires each of the three major U.S. consumer reporting
agencies to provide you with one free copy of your credit report every year. Be a cautious, proactive consumer, and you can easily avoid becoming an identity theft statistic!

Get prepared for the Privacy War!