

Protect Your Privacy

Personal information is much more than just your name, address and passport number, it is a valuable part of who you are, and you should treat it with respect.

This guide to protecting your privacy comes from the makers of **Erasing David**, a feature documentary about civil liberties and the database state.

Some of these actions can be done in a matter of minutes, most require a slight change of thought, all are beneficial in claiming back the control of your personal information.

For more details about the film please visit www.erasingdavid.com

**ERASING
DAVID**

What is Privacy?

Personal information is much more than just your name, address and passport number. It includes records of your shopping habits, your driving record, medical records, work history, credit score and lots more. The information can be stored by many private and public organisations including your place of work, school, local council, bank, travel agent, police department, the list goes on...

Having a **right to privacy** means you can control this personal information. That means you have the right to demand that you consent (agree) when this data is stored - this gives you the ability to limit who has this information, how this information is kept and what can be done with it.

Basically, another way of saying that you want a right to privacy is to say you want **CONSENT** and **CONTROL**.

But what you must know - and watch **ERASING DAVID** if you don't know this - is that **personal privacy is given away voluntarily, unknowingly, lost, bought, sold or stolen every day.**

Pretty much any interaction with a government, corporation, or online can be privacy reducing:

- Buying groceries and services electronically
- Giving money to charity
- Visiting the doctor
- Social Media sites
- Joining a society
- Using a loyalty card
- Taking out a mortgage

For companies, data is very easily converted into profit. Knowledge is power - it allows companies to market more effectively and to mine data about current and potential customers.

Government departments create birth, death and marriage certificates, monitor benefit transactions and store court records. Governments increasingly are learning from companies that the more you know about the customer (in this case, the citizen) the more you can dictate, cajole and control.

Try searching your own name online. There are now information brokers who package and sell any of this information that is 'public' (which means you didn't read the small print and didn't opt out) to anyone interested.

Then there's **data loss and malicious stealing.** Data breaches are causing concern when the personal information of millions of people is being compromised.

We have produced this pack as an extension of the film ERASING DAVID to give you tips on how to Protect Your Privacy with regards to Commercial Companies, Governments and the Internet. This guide is the tip of the iceberg when it comes to safeguarding your personal information and we highly recommend that you take a look at our partner pages for further, and more in depth information about issues of civil liberties.

Come on, who really cares? I've got nothing to hide...

That's the thing. **You don't value privacy until it's gone.**

Ask anyone who has been the victim of identity theft. Lost privacy normally means years dealing with harassing debt collectors, police, credit agencies and government departments.

Victims of stalking and harassment find that the brave new database world means that there is no place to hide - because all our electronic footprints and past data wakes make it very hard to live and work without creating a record that can be traced by a web-savvy stalker.

But for everyone, lost privacy means your personal information (likes, dislikes, habits) is collected, analyzed and shared by marketers, employers, insurance companies and the government without your knowledge or consent. On a basic level you will find this out when you suddenly get a pile of junk mail or cold calls, but this could also mean you are refused a job after someone looks at your social networking profile or you are denied insurance because of previous unrelated claims on different policies.

The law will protect me though...

There are a patchwork of laws covering different types of data protection - with, for example, separate bits of laws for medical privacy, financial privacy, telephone privacy, email privacy and credit privacy. But these are often completely undermined by new overarching anti-terror laws enacted in the last ten years. We've been scared into accepting these without really considering the downsides for us as individuals.

There are a lot of big holes. Technology constantly evolved, and the law cannot keep up. It is up to us.

What shall I do?

Educate yourself. Learn how to **Protect Your Privacy**. Watch **Erasing David**. Follow the guides we're bringing out. We are not affiliated to any of the services we mention here. And if you join our email list, we hope it goes without saying that we will never share your details - we don't even want to know your name. In fact, why not set up a new anonymous and secure email address and use that to subscribe to this, and other sites where you don't want your details known...

Support legislation that defends privacy. Oppose legislation that reduces it.

Don't do business with companies with poor privacy practices. You know who they are... If you don't - read the newspapers.

Simple steps to being a Private Citizen

- Look after your Rubbish** **This was the first way that private investigators, Cerberus, were able to start profiling David in the film.** Shred paper that has personal details on it and when you throw away or give away a computer, wipe the hard drive so that no trace of personal and business stuff remains. To do this you need to either physically destroy it or polish it clean with a suitable program. Deleting data is not good enough for even the most inexperienced thief. There are programmes here that do this: <http://epic.org/privacy/tools.html>.
- Lock it away** Store all of your personal information in a secure place within your home. If, in the unfortunate circumstance, your household suffered a burglary, you would be worse off them stealing your credit card number and birth certificate than physical material goods.
- On the Internet** **You wouldn't give out personal information to a stranger in the street, so why are you happy to do it online?**
- Don't send any personal information that could be sensitive and you are not happy being known by the whole world (e.g. phone number, password, address, credit card number, secret word) by email, or by online chat, instant messages, forums, or in any online profile. Your messages are not private unless encrypted.
 - Avoid giving your real name wherever possible, and create a fake email address for mandatory fields.
 - Set your browser to let you know when cookies are installed. These are application which store information about your such as username and passwords. Don't ever use cookies on public computers.
 - Remember that mail applications can be accessed by other people. There are strict laws about bugging or tapping into to personal mail but just because it is illegal, doesn't mean that it won't happen.
 - Be cautious when using public wi-fi networks, which may be insecure and therefore accessed by other people.
- Phone** Block your caller ID. **Never give out personal information over the phone unless you are certain who is on the end of the line.** If you are suspicious, take their name, hang up and try to call them back on their switchboard / main phone number.
- Cash Cards** **Shield your PIN** when withdrawing cash and check that there is no-one near you. Don't start tabs in bars or restaurants where you card will be left unattended, always accompany the waiter to the till or request a card machine at the table. Cards can be easily swiped and copied within a few seconds.
- Social Networks** Check your **privacy settings** on all your social networking sites. Do you really want the whole world to see and be able to comment on a picture of you and your friends on a big night out? Why not restrict your Facebooking to friends and family only?
- If you are over the whole social networking thing there is a way out. Suicide Machine is a free service that closes and deletes all your online social networking accounts. You will probably save some time, definitely protect your privacy and perhaps even start speaking to your friends in person again... <http://suicidemachine.org>

Don't become part of the marketing machine

Direct Mail and Tele Marketing

Want to stop direct marketing mail clogging up your doormat? Join the Mail Preference Service now. It takes 1 minute: www.mpsonline.org.uk

By registering with the MPS, direct mail companies are informed not to send unsolicited mail to your door unless you have given individual permission to that company. Check out the tick boxes at the end of each form you sign to approve or deny that right. The boxes are usually small and hard to find, but necessary unless you want an endless stream of paper coming through your door.

While you are there also register with their Telephone Preference Service for a quieter life without any nasty sales calls becoming a nuisance in the evening. It's completely free and takes no time. www.mpsonline.org.uk/tps

If you receive regular unwanted mail from a specific company despite being registered with the MPS, you have probably forgotten to tick the opt-out box. To stop such mail you have to contact the sender directly and ask to be removed from its mailing list. By law, organisations are obliged to respect such a request. Never say people can share your data. If you forgot when you signed up with a company, just send them a letter or email saying;

"Dear Company, please note that I do not want you to use any of my personal data for any purpose other than to provide me with your service and bill me. Never share my details with anyone else. Thanks."

When you provide your name, address, phone number and other personal information, your name could easily end up on mailing lists. Here are the classic examples:

- Warranty and product registration cards. Give nothing - you'll be covered anyway.
- Joining an organization or club or charity - or giving them money. Tell them (and write on the direct debit form / letter) never to sell or exchange your name with anyone.
- Starting any subscription. Tell them never to sell your name.
- Don't list your phone number & address in the phone book

Freebie Competitions

Avoid these because they flag you up as an "opportunity seeker" - or a "gullible". Opportunity seekers are to marketing people what ripe peaches dipped in honey are to wasps. Contests (and any get-rich schemes) exist to harvest names and addresses of gullibles. Don't be one.

Loyalty Schemes

Cut up your loyalty cards. The money off is not worth it. Supermarkets make far more from selling and using your data than they give back to you in money-off vouchers. You'll shop in more varied places and save money. If you shop online then be aware the most major supermarkets will keep you data whatever you set your preference to. So we say don't.

In London, get a new Oyster card (£3 deposit) and don't register it. Alternatively swap Oyster cards with friends to confuse the system.

DVLA

Get a copy of your driving record. In the film David discovered that a long-expired driving offense was still on his DVLA record 14 years on. Anyone can see that.

To get release of information about yourself send a letter to:
DCS (Data Subject Enquiries), D4, DVLA, Swansea SA6 7JL.

Give details of your address, driver number or full name and date of birth. You have to give a reason for request. David said it was, "*because I want to know*". A fee of £5 is payable.

Credit Report

Get your credit report. New government measures mean that by June 2010 you will, by law, be able to access your basic credit report online with the three main agencies at a cost of £2. (Until now, the agencies only have to offer £2 reports by post). Equifax is already offering this facility which you can access here:

<http://www.equifax.co.uk/Products/credit/statutory-report.html>

Experian and Callcredit will follow suit by June. People who are receiving debt advice or are victims of identity fraud will be able to access this kind of report for free. However, these types of reports are fairly basic. It is simply a copy of the information available to banks and lenders held about you, plus guidance on how to understand it and, where appropriate, resolve any issues. You can get more detailed reports that give a full list of your credit agreements, but you will most likely have to sign up for a monthly subscription for these types of reports. The prices vary from £6.99 a month for Equifax, £7.99 a month for Experian and £12 a quarter for Callcredit. Consumers can take advantage of 30-day trials with the monthly services by signing up, checking their credit report and then cancelling before they are charged. The Callcredit service, however, take the first payment when you sign up.

Fight against the Database State

Medical Records

You like to think that a massive database with all our health records on is a good idea. But you'd be wrong. Now is the time to opt out. Once your records are uploaded, you've no chance of getting any kind of control over them ever again.

Even GP's are warning against the database as they fear that patient's rights are being overlooked. <http://www.guardian.co.uk/society/2010/mar/07/nhs-database-doctors-warning>

This website delivers a good argument for opting out, and writes the letter for you in around 30 seconds. You do have to press print and then sign and post it.

The Big Opt Out <http://www.nhsconfidentiality.org/optoutletter>

ID Cards

Let's get this straight — it isn't just about identity cards. The government's identity scheme includes a huge database to keep tabs on everyone, a massive infrastructure to collect peoples' details, and a giant network of technology required to verify people against their cards and both of these against the database.

This will be the largest accumulation of data by the state, including our biometric data as well as just names and addresses. There is no case that this loss of liberty will lead to an increase in security in the UK. If anything the introduction of ID cards could lead to higher security risks through access to a centralized database and identity theft.

The main problem is that all systems have errors. Personal information will be controlled by the state, who will be able to access and change profiles at the click of a button without the need to contact the individual.

Sign the NO2ID pledge www.no2id.net

How do I find out what is already out there?

During the making of ERASING DAVID, David applied to all the companies and organisations he had ever been in contact with to request what they knew about him. The level of detail and quantity of information returned was astounding. Every citizen has the right to apply for this information for themselves by using the Data Protection Act, which gives you the right to know what information is held about you and sets rules to make sure organisations handle your information properly. It is important that you make sure that information is correct and in responsible hands, otherwise you may get into difficulty.

Making a **Subject Access Request** is simple and requires a response by law within 40 days. Write a letter to the company secretary including your;

Full Name

Full Address

Any information that certifies who you are to that organisation.

After they have replied, if there is a mistake, you should respond with any corrections immediately. If you feel that the company is not acting in accordance within guidelines you may report them to the **Information Commissioner's Office**, an independent public body set up to promote access to official information and to protect personal information.

Data Protection Act 1998 – gives you the right to know what information is held about you, and sets rules to make sure this information is handled properly.

Privacy and Election Communications Regulations 2003 – set rules for people who wish to send you electronic direct marketing via email or text messages.

Freedom of Information Act 2000 - UK government legislation defining what information public sector organisations are obliged to provide on request.

Please see www.ico.gov.uk for further information on these laws and how they affect your rights.

In General

Be **strong-minded** and **assertive** when anyone asks for personal information from you - especially if you suspect that it is not necessary.

Tell anyone that has your name, address, phone number and email address that you do not want your information shared, rented or otherwise released.

Verify requests for information, especially if it is sensitive - like your mother's maiden name. By the way, it is a really good idea to have a fake mother's maiden name. But you will need to remember who you've given it to.

Find out whether the information they're asking for is **necessary** or **voluntary**. Give the minimum.

Ask **why** they want it and **how** it will be used.

Ask how long they keep information and when it will be **deleted**.

Remember, lots of companies never delete their data.

Further Information

NO2ID – www.no2id.net

Liberty - www.liberty-human-rights.org.uk

Action on Right For Children - www.archrights.org.uk

Independent Commissioners Office – www.ico.org.uk

Henry Porter blog - <http://www.guardian.co.uk/profile/henryporter>