Take Back Your Online Privacy User's Guide 2025

Author Hugh Cull, Digital Privacy Expert

Feel free to contact me: hugh.cull@copc.ac.uk. Updated May 2025

Table of Contents

Feel free to contact me: hugh.cull@copc.ac.uk. Updated May 2025

What is the difference between Security and Privacy?

Security is referring to how you protect yourselves and your property. Privacy refers to how you control who has access to your personal information and how much access you allow them to have. People often assume security and privacy are the same thing, they are not! Your online privacy is very important to protect because you are not just protecting your privacy but that of your children, family, and friends.

I do not care about online privacy as I have nothing to hide!

When I discuss online privacy, I often hear the statement "**I do not care about my online privacy**". It is not about having something to hide it is about having something to protect. Don't confuse privacy with secrecy. Everyone has some personal information that they wish to protect. Would you be happy to share all your personal information with a stranger who might pass this information on to others?

Arguing that you do not care about the right to privacy because you have nothing to hide is no different from saying you don't care about free speech because you have nothing to say – Edward Snowden.

Privacy is closing your bedroom curtains when getting ready for bed. Privacy is visiting with your doctor behind closed doors. While in real life this type of privacy comes naturally, with little thought, in the digital space the idea of privacy is skewed. Mostly because people don't really understand what digital privacy entails. You have a passcode or some sort of security on your phone. Same goes for email. Nobody ever handed me their phone to allow me to read their chats or see their pictures. If you didn't have anything to hide, you wouldn't care. But you do. Everybody does. **Privacy is something that makes you human**. Privacy gives you control, of your life. Privacy makes you a human with control of your personal data. Without privacy you are just a commodity to be controlled, manipulated, discriminated, and repeatedly sold.

Privacy is a basic human right. It is so important to your wellbeing that it is enshrined in the Human Rights Act 1998, article eight and article twelve of Universal Declaration of Human Rights.

Why is online privacy important?

Many people underestimate the importance of online privacy, but they should be aware of how much information they're sharing, not just on social networks but just through browsing itself.

The importance of digital privacy becomes clear once you try to make a mental list of personal things, you're ready to share with complete strangers and those you'd rather not.

For sure, you don't want your medical records, bank statements, or even certain items from your shopping cart to be widely known. You may not be aware of how easy it is for people to get hold of someone's personal information like home address, friends' names, tastes, or favourite places based on what they publicly shared. A lot more personal information on not just them but their whole family.

Yes, you can make your social media account private and share only specific content with a specific group of people (although the social media platforms save and share all that data you think is private). But how can you really know what social media does with the data you share? And what about your other online traces, like browsing history, searches, purchases, or even your online correspondence?

With the popularity of smartphones and the apps installed on these mobile devices, data harvesting has gone to a new level. Many apps request location details, usernames, phone numbers, or email addresses. Yet, some go further and ask you for risky permissions, information that could cause trouble if it fell into the wrong hands. It could be access to your phone's microphone/recorder, camera, contacts, or even all the data on your smartphone.

These data harvesting tech corporations are recording every aspect of your family's lives every second of the day. Taken together, all this information can be used for "profiling" or making a customer persona based on the person's browsing, shopping, and social media preferences, education, political views, sexual orientation, religious beliefs, health, and many more personal categories. This profile can then be used to discriminate against you and your family, now and in the future. We all want to keep our family safe especially our children, but this is not possible without taking control of your online privacy.

People may assume it is all about what they are doing, which is a small piece of the picture. However, online privacy has less to do with what you are doing, and more to do with who you are AND what you are doing. On the Internet, data has high value. It’s stolen, sold, collected, and analysed.

There are many facets to privacy. There’s what you do, and who you are. Who you are is your personally identifiable information (PII), which is as it sounds, your name, date of birth, address, Social Security number, phone numbers and more. What you do are the searches you perform, the websites you visit, the articles you read, even what you buy online.

Whenever you download an app, visit a website, or use a social media platform, chances are that company is collecting data on you. People are doing so much more online through their computers and mobile devices today. We make purchases, look up medical conditions, arrange holidays, interact with friends and relatives, just about anything imaginable. With these actions, people are inadvertently creating a huge digital paper trail of data about themselves. **This personal data will be stored online forever**.

Identity theft is nothing new. It has been a crime long before the internet. But new technology has opened fresh avenues for con artists, cyber criminals, and sexual predators. With all this personal data available it is easier than ever for them to find their next victim.

My online data is not worth anything!

The reality is that you are worth a lot more than you think. The most valuable commodity on Earth used to be Gold. **Data is now the most valuable commodity on Earth.** A complete data set on an individual can fetch a vast profit, completely legally, too. There are now companies known as “data brokers” that collect and maintain data on millions of people, which they analyse, package, and sell without the user’s knowledge or permission. Data brokers make billions of profits from harvesting and selling your family’s data. This is a billion-dollar industry and by 2035 will be a trillion-dollar industry. Data brokers know more about your family than you think and do more with this data than you would like. Scammers buy this data from data brokers to find and create bespoke scams that are more successful as they know so much about your family there is a greater chance you will fall for the scam. Using your family’s data, they can see what emotional buttons to press to get you to fall for the scam. The scammers know emotions cloud judgement. For example, they will target a loved one who has recently lost a family member from the funeral data available online. The less you care about your family’s digital data the more scammers may target you. Your family’s privacy is so important to protect. You and your family are just a commodity to be controlled, manipulated, and monetised. However, it does not to be this way if you know how to protect your family's online privacy.

I do not share that much personal information online!

Your data is being harvested every second you spend online. It is not just your online data but your offline data as well. The sheer scale of this data harvesting is insane. I have spent years researching how much personal data is harvested from online users and it is immense. Most users are totally unaware of the amount of personal data that is available to these unregulated corporations.

Below is a list of the data these organisations may know about you and your family.

- Every location you have visited.
- Every website you have visited and your search history.
- Your age, gender, hobbies, career, interests, and relationships.
- Every app you have used, how often you use them and who you interact with (including Facebook data).
- All your viewing history on You Tube.
- Your websites you have bookmarked.
- All the data from your phone including voice conversations.
- All your email messages.
- Every event you have attended.
- What you and your friends like and dislike.
- All your contact information online and in your phone.
- All your data stored on Google Drive and OneDrive.
- Every image taken on your phone.
- All the data in your calendar.
- The music you listen to.
- Conversations in your home and on your phone.
- Your exact location anywhere in the world.
- Every file you have ever been sent or viewed.
- All the data from apps on your phone.
- Some or all your health data.
- Where you shop and how much you spend.
- Data you share on WhatsApp and Instagram.
- Data extracted from your family, children, and friends.
- What you and your family & friends look like and sound like.
- What you watch on TV and in the cinema.
- Your religion and political allegiances.

- How much wealth you have including pension information.
- Your complete work history and qualifications.
- Every magazine and newspaper you have read.
- How much exercise you undertake.
- Your children's location, age, school, and academic history.
- Your criminal record or any criminal incident you are involved in.
- Your bio metric data (fingerprint – face and voice).
- Data from questionnaires you have completed.

This is just a fraction of the data they could have on you!

Your online data and that of your family tells a vast amount about your life, your values, your weaknesses, your daily routine online and offline, and so much more.

All this data is used to create a social profile of you and your family. Every day the data in this social profile is updated and the more data in your social profile the more it is worth. This data is used to predict your behaviour and the more data in your social profile the easier it is to control, manipulate and monetise you and your family. This data predicts not just which shirt you might be willing to buy, but which topics are so emotionally charged you cannot look away from them and which pieces of propaganda will work best upon you. This makes the platforms that collect data at scale, a cunning way to influence human beings.

What are the consequences of my data being shared?

This data is available to anyone who wants access to it including criminals, cyber criminals, stalkers, ex partners, health companies, insurance companies, mortgage companies, credit companies, recruitment companies & governments to name a few. The more of your data that is harvested the greater your risk of cybercrime. The more of your data that is harvested the more of your privacy is eroded. From analysing your data any company can use this information to manipulate you or use this data to discriminate against you or your family. The big data harvesting tech corporations see their users as a commodity to monetise for profit.

Recruitment companies use all this personal data of potential candidates to decide if they should invite them for an interview. Every action and comment you have ever shared online can be seen by potential recruiters and this vast amount of data will be used to judge you. Think about how young people share so much information online with no idea of how that data will be used to judge them in the future.

Medical insurance companies can use all your harvested data to decide if they should increase your premium, not insure you or refuse your medical claim.

Online and offline companies can use the vast amount of data about you and your family to charge you more for their products or refuse to sell to you anything if there is a characteristic of your personal data they do not like (sexual orientation or religion for example).

Credit companies use your data to decide what rate to charge you or to refuse you a credit card or any form of credit. This applies to mortgage companies and credit rating organisations. People may find they can't rent any properties due to all their personal data being available to judge them.

Using Artificial intelligence software (AI) and your family's personal data available on the Internet you can receive a phone call where you hear your daughter or sons' voice saying they are in a dangerous situation and need money urgently. The voice you are hearing is not your daughter or son but AI using your family's data to mimic their voice. Using your family's data allows these scammers to create AI voice scams more realistic and this increases the chance you will fall for them. These types of attacks are becoming very popular with scammers as they are so successful. The more of your family's data available online the greater risk you will receive these types of phone or video scams.

Companies are dreadful at keeping your family's data safe. No company is safe from being hacked and their customers personal data being acquired and sold. There are two types of companies, those that have been hacked and those who do not yet know they have been hacked. It is so important people start to care about what data they put into the Internet connected world. The best way to protect your family is to stop using data harvesting technology corporations. Instead replace these corporations with those who focus on protecting your family's personal data. Covered later in this guide.

I recommend reading **Shoshana Zuboff** award winning book called **The Age of Surveillance Capitalism** for an in-depth analysis of the dangers of this new type of capitalism.

Case Study one:

Microsoft will pay $20m (£16m) to US federal regulators after it was found to have illegally collected data on children who had started Xbox accounts. The company also failed to inform parents about all the data it was collecting, including the user's profile picture and that data was being distributed to third parties.

Case Study two:

Google Violating Child Privacy Laws. In 2019 YouTube was fined 170 million dollars for violation of privacy rights of children. YouTube, a company owned by Google, was found to have gathered children’s data without their parents’ knowledge or consent and violated the Child Online Privacy Protection Act (COPPA).

Case Study three:

Ring Doorbell Trackers. Ring Doorbell is an app that allows you to see and speak to someone who comes to your doorsteps when you are not home.

Unfortunately, the app is absolutely packed with 3rd-party trackers, an investigation by the Electronic Frontier Foundation discovered.

According to the EFF report, Ring Doorbell sent personally identifiable information (PII), including usernames, IP addresses and data from device sensors to facebook.com, appsflyer.com, branch.io and mixpanel.com.

By installing a Ring camera, you allow Amazon to spy on your neighbours and with the built-in microphone hear all the conversations in the road that are within range of the microphone.

Case Study four:

A young woman purchased a few nondescript items such as cotton balls, unscented lotion, and some vitamins. Based on what the company already knew about her, they were able to correctly predict that she was pregnant and began targeting her for baby items by sending her coupons in the mail. The issue? She was a teenage girl, and these coupons alerted her father (much to his dismay) that she was indeed pregnant.

Case Study five:

Due to privacy concerns, Google's location-tracking practices have come under intense scrutiny in recent years. The company tracks the location of its users, even when they have not given explicit permission for their location to be shared. This revelation came to light in 2018 when an Associated Press investigation found that Google services continued to store location data, even when users turned off location tracking. This was a clear breach of user trust and privacy, and Google faced significant backlash from users and privacy advocates. Google was fined 300 million dollars for selling location data from users.

Case Study six:

Amazon agreed to pay 25 million dollars after the Federal Trade Commission found that it had retained sensitive data, including voice recordings of children, for years.

Case Study Seven:

Instagram and Facebook parent company Meta purposefully engineered its platforms to addict children and knowingly allowed underage users to hold accounts, according to a newly unsealed legal complaint.

The complaint is a key part of a lawsuit filed against Meta by the attorneys general of thirty-three states in America late October 2023. The lawsuit alleges the social media company knew, but never disclosed, it had received millions of complaints about underage users on Instagram but only disabled a fraction of those accounts. The large number of underage users was an “open secret” at the company, the suit alleges, citing internal company documents. The lawsuit also focuses on longstanding assertions that **Meta knowingly created products that were addictive and harmful to children**, brought into sharp focus by whistleblower Frances Haugen, who revealed that internal studies showed platforms like Instagram led children to anorexia-related content. Haugen also stated the **company intentionally targets children under the age of 18**.

Company documents cited in the complaint described several Meta officials acknowledging the company designed its products to exploit shortcomings in youthful psychology, including a May 2020 internal presentation called "teen fundamentals" which highlighted certain vulnerabilities of the young brain that could be exploited by product development. The presentation discussed teen brains' relative immaturity, and teenagers' tendency to be driven by "emotion, the intrigue of novelty and reward" and asked how these asked how these characteristics could "manifest in product usage".

Case Study Eight

In 2021 Meta changed its privacy policy to state that Meta would start to share WhatsApp data with third parties. The Competition Commission of India is fining Meta $25.4 million, saying it shouldn't have required WhatsApp users to share data that they thought was private.

Can you guarantee that your data will not be used against you in the future?

We have no idea who will be running this country in the future and how they will use your data. No one can guarantee that their social profile will not be used against them. You just have to look at America for an example of why your privacy is important. The Supreme Court banned the rights of women in America to have an abortion. There is now evidence that the states that are upholding this law are accessing the data of all their residents to track those who may be pregnant or those who have visited an abortion clinic. Data from Google, Facebook, Period apps and other data harvesting services are now being used to take control of those people and force them to go ahead with the pregnancy. As I have already said you have no idea how your family's personal data will be used against them in the future.

It is important that people start to take steps to reduce the amount of personal data is being harvested and added to their social profile. The most important thing to remember about your privacy is that it is **YOURS**.

This is sad but true that some people have forgotten how important it is to protect their personal data and liberty instead have sacrificed their privacy for convenience. People tell me all the time they love the convenience of technology. The problem is that they are unaware of the personal cost to their family's privacy and safety of this convenience. Convenience is the enemy of privacy.

Once you have lost your privacy, you realise you've lost an extremely valuable thing. Privacy is a right, please don't let it become a luxury!

Feel free to contact me: hugh.cull@copc.ac.uk. Updated May 2025

The concern of privacy advocate like me is that we could be witnessing the death of privacy in society. No one wants their children to grow up in a world where they will have no privacy. Where they are a commodity to be bought and sold. Where they are continually discriminated against and judged. Is this the world you wish to live in?

Who are the biggest data harvesting organisations?

Google, Amazon, Facebook & Microsoft.

These organisations harvest your data on an industrial scale. They go to extreme lengths to manipulate their users into sharing every aspect of their family's life. The first step to claiming your privacy back is to remove these data harvesting organisations from your online life. It is possible and I will discuss how to do this later in this guide.

Google

Google is the king of data harvesting as it harvests vast amounts of personal data from its users. Its software is cleverly designed to get access to every aspect of a user's life. Virtually every mobile phone (apart from Apple iPhones) run Google operating software giving Google access to user's personal information on their mobile phones. Google has trackers on virtually every website so it can track which websites people view, and its search engine is designed to harvest every search query entered. All Google products are designed to invade the user's life and gain access to their personal data. Google still read your email messages and retain access to your inbox. Additionally, by using Gmail and remaining logged into your Google account, your identity is associated with everything else you do while using Google products, including Search, Maps, YouTube, and more. Google keeps a dossier on its billions of users sourced from a dizzying number of sources. They have software in schools (Google Classroom) so children will see Google as a corporation they can trust. From its operating software, smart (surveillance) speaker, smart watch, Chromebook, in car software, search engine, Chrome browser, cloud services, YouTube, Google Play store, Google AdSense, Google analytics etc., it has access to virtually every aspect of a persons and their family's life. People naively trust Google with their personal data with no idea of how this corporation profits directly from its user's data. **Google is surveillance by design.** Google is repeatedly fined billions of dollars for severe invasions of user's privacy, yet they keep on harvesting and sharing their user's data. These are massive amounts, but they don't seem to have had any appreciable effect on Big Tech's behaviour. That's because these fines, massive as they are, represent little more than an inconvenience to these companies. It seems that Google, and others view these fines as the price of doing business and will continue to pay these astronomical amounts if it means they can continue abusing your data and crushing alternative business models.

You are NOT Google's customer you are the commodity Google sells to its customers.

In the first seven months of 2023, Big Tech companies have been fined nearly $2.34 billion for privacy violations and abusing their monopoly power. Since the European Union introduced the GDPR in 2018, these companies have been fined upwards of $7 billion.

Meta (Facebook).

Facebook announced to change its parent company name to "Meta," offering social media products including Facebook, Messenger, WhatsApp, Instagram, Oculus, and others. However, the users' online data and privacy is still a big issue due to the company's checkered reputation for security breaches and data collection. It has been fined billions of dollars over the years for **severe** invasion of its users' privacy.

Just recently Facebook paid more than a million Americans at least $345 for collecting data without their consent. Facebook reached a $650 million settlement (largest settlement in US history) of claims it collected and stored millions of users' biometric data without consent. The big issue with your biometrics is that you can't change your biometrics like you can your password.

Each time Facebook finds itself embroiled in a privacy scandal, the general playbook seems to be the same: Mark Zuckerberg (CEO) delivers an apology, with recycled lines, such as "this was a big mistake," or "I know we can do better.". When you make billions from selling your users data the fines for severe invasions of their privacy mean nothing to Meta's bottom line. For Meta is all about profit and collecting enough of your users' data to achieve this. The less privacy your users have the more profit Meta can make.

Social media platforms like Facebook go to extreme lengths to harvest all the data about you and sell access to it. Facebook will use any method to extract personal data from its users as its users are just a commodity to be bought and sold. Their social (surveillance) platform is the perfect platform to harvest all the data from its users. This company profits from the knowledge that someone has a disease, or has lost their loved one in an accident, or has been a victim of rape.

Facebook is the world’s second most toxic surveillance platform on planet Earth (Google is the first). Its own internal research highlighted the damage its products are doing to the mental health of its users. **There is NO privacy when you post personal information on Facebook**. All the data is harvested and analysed by Facebook and anyone who is willing to pay can have access to this data. Facebook is so confident in its understanding of people and their preferences (from the vast amount of data it has on its users) that Facebook can essentially guarantee a certain number of people will do certain things. From the vast amounts of data, it has on its users it can easily manipulate them into doing whatever Facebook wants them to do.

From the testimony and evidence of whistle-blowers that worked at Facebook we know the power of manipulation that Facebook has over its users.

Privacy advocates around the world state:

Facebook isn’t so reputable when it comes to users’ data privacy. From poor data management to shady data-sharing and monetization, Facebook has been found involved in numerous malpractices.

Remember even the founder and CEO of Facebook, Mark Zuckerberg does not let his family use Facebook or any Meta services.

“***Facebook, just like big tobacco companies before it, had known the toxic truth of its poison, and still fed it to us***”. Whistleblower and former Facebook employee Frances Haugen 2023.

Don’t make the mistake of thinking you’re
Facebook’s customer, you’re not.
You’re the product.

According to state attorneys general from forty-two states in America, Mark Zuckerburg not only knew that Instagram (part of his company Meta) was harming children; he continued to allow it to operate as before even when warned by his own staff.

I have spent many years researching the privacy issues with Meta and all its products, and I could fill many pages with the privacy issues and nefarious data harvesting practices that make the corporation so toxic to its user’s privacy and safety. Meta is as addictive and dangerous to all its users as cocaine.

Amazon

Amazon is quickly becoming the third most successful data harvesting corporation on planet Earth. Amazon also has trackers on virtually every website to spy on you, but amazon acquires a lot of your personal data for its smart (surveillance) devices like Amazon Alexa and Ring doorbell. You are encouraged to link your Amazon Alexa to other devices in your home so all your personal data will flow through Amazon Alexa and onto Amazon's servers. You may think you are in control of the data from these smart (surveillance) devices, but the reality is that you have limited control over the data it sends back to Amazon. It is not just customer privacy concerns, but their labour practices are appalling, and they asset strip the competition as well as poor security procedures to protect their customers data. This came to light through information shared by three former high-level information security employees. Amazon has recently been fined $877 million dollars for invading user's privacy. Please don't shop on Amazon, instead support more ethical companies. They are often cheaper than Amazon.

Microsoft

Windows 10/11 users have more than just updates that break things and critical security warnings to worry about. There's also the important matter of user data privacy to consider.

When you install Windows 10/11, Microsoft forces you to give them a lot of personal information before you can complete the installation. They even force you to create a Microsoft account before you can use the operating system.

The Dutch Data Protection Agency (DPA) has been testing privacy protection changes to the operating system and they were quoted as saying:

The average Windows 10 user will likely click through the privacy notice without really understanding what that data will be used for. It was this "unpredictable processing" that was at the heart of the DPA investigation. "The way Microsoft collects data at the full telemetry level is unpredictable," the DPA said at the time, "Microsoft can use the collected data for the various purposes, described in a very general way." It was that lack of transparency, along with a multitude of data collection purposes, that the DPA argued meant Microsoft couldn't "obtain legal ground, such as consent, for the processing of data."

Microsoft Windows 10/11 data gathering practices became so controversial that the French government stepped in and ordered the software giant to stop tracking French users. Even the Electronic Frontier Foundation (EFF) blasted Microsoft for disregarding user privacy and choice with Windows 10. Windows 11 is even worse for its data harvesting practices.

The operating system sends back to Microsoft vast amounts of data that has nothing to do with the operation of the software.

Federal German data protection authorities have banned the use of Microsoft Office 365 in schools due to privacy concerns around the use of US cloud providers (January 2023). A better and more private alternative to Microsoft Office is Libre office.

The German Data Protection Conference said that, given the lack of transparency around how Microsoft collects and processes personal data, as well as the potential for third-party access to it, the use of Office 365 is not legally compliant with the General Data Protection Regulation (GDPR).

The GDPR stated "Microsoft does not fully disclose which processing operations take place in detail. In addition, Microsoft does not fully disclose which processing operations are carried out on behalf of the customer or which are carried out for its own purposes,"

After first highlighting other privacy concerns relating to user's personal data two years ago, Microsoft has not resolved any privacy compliances issues with its office products.

On October 14th, 2025, marks the end of support for Window 10. Microsoft will no longer offer security updates, technical support or software updates. Microsoft has increased the hardware requirements for computers to run Windows 11 forcing users to purchase a new computer just to run Windows 11. Millions of perfectly good computers (over 240 million) will be scrapped for no reason except Microsoft dictates it. This will increase the E-waste problem the planet already has. However, all those computers will run security and privacy focused Linux operating system perfectly OK.

Is there a privacy alternative to Microsoft Windows?

Linux is a privacy-based alternative to Microsoft Windows and is used by millions of people around the world as well as business's and is used in critical industries. has gained popularity for its flexibility, security, and cost-effectiveness. It's a powerful alternative to Windows and macOS, and it's worth considering as the end of Windows 10 support approaches.

There is no need to create an account to use Linux and it is easier to use than Microsoft operating systems and is ideal for all levels of computer user. I have been using Linux for several years now and I assist people to migrate from Microsoft to Linux. Contact me if you would like a demonstration of Linux or to discuss migrating over to a more private, reliable, and secure Linux operating system.

An operating system does not need to send back vast amounts of user's data to operate. Linux works just fine without any data harvesting.

Linux is so secure, reliable, and private that Google, Facebook, and other corporations use it to run their servers. Linux is the perfect replacement for Windows 10/11.

Privacy facts about smart (surveillance) speakers and smart watches:

In 2020 a Google update to its smart speaker products caused them to start recording when any sound was heard in the room.

Amazon & Google has spent billions on making its personal assistant sound more human so we will trust it and share more personal data. Remember these tech companies directly profit from the voice conversations from smart speakers.

John Simpson, Consumer Watchdog's privacy and technology project director, said: 'Google and Amazon executives want you to think that Google Home and Amazon Echo are there to help you out at the sound of your voice. 'In fact, they're all about snooping on you and your family in your home and gathering as much information on your activities as possible.

When connected to other devices in the home allow more data to be shared with third parties. Also, ability to track a person's movements. Data collected through smart speakers can be combined with data from other sources, creating fine-grained user profiles.

Amazon Sidewalk now connects Amazon smart devices to each other using the 900MHZ range so they can communicate with each other over a wide range. This allows Amazon to track people who are not running any Amazon smart devices. Users are automatically opted into this by Amazon. Users are aiding Amazon to spy on their neighbours.

The UK's National Health Service (NHS) has signed a deal for medical advice to be provided via the Echo. At face value, this simply extends ways of accessing publicly available information like the NHS website or phone line 111 – no official patient data is being shared.

But it creates the possibility that Amazon could start tracking what health information we ask for through Alexa, effectively building profiles of users' medical histories. This could be linked to online shopping suggestions, third-party ads for costly therapies, or even ads that are potentially traumatic (think about women who've suffered miscarriages being shown baby products).

These smart devices are designed to record your conversations and add these to your social profile. Ask yourself, would you be comfortable for everyone to listen in on every conversation you have at home or outside your home? To have all those conversations recorded and available for anyone to listen to. Most people would not like the Government to mandate that they must have a tracker in their home or attached to their wrist, yet people purchase and install these devices in their home or on their wrist.

The Amazon ring doorbell is another way Amazon can spy on your neighbours. As one expert from US privacy org the Electronic Frontier Foundation put it, "Ring has steadily been becoming one of the largest surveillance apparatuses in the nation”.

There have also been reported data leaks and concerns that the Ring Doorbell app is full of third-party trackers (including Google and Facebook) tracking a good amount of personal information that Amazon Ring doesn’t disclose.

In October 2021 A judge ruled that a doctor's neighbour's Ring smart doorbell cameras breached Dr Mary Fairhurst privacy in landmark case. She told the court that Amazon-owned Ring cameras placed her under 'continuous visual surveillance'. Judge Melissa Clarke found the Ring camera breached provisions of the Data Protection Act 2018. Remember the Ring camera doorbell also has a microphone that can record all conversations. Over the past few years there have been many security issues found where hackers can gain access to the Ring doorbell’s data and access the home’s wireless network and gain access to all the devices connected to the house Wi-Fi network.

If you are having a conversation with your friends or neighbours near the Ring doorbell this conversation will be recorded and sent to Amazon.

The more devices you connect to your home network the greater the risk of attack. These devices have poor or no security and are an easy target for cybercriminals. Once a hacker has gained access to your smart speaker, they can easily access your whole home Wi-Fi network, and all the devices connected.

Remember the word SMART really means SURVEILLANCE.

Smart Meter Privacy Risk

The government is keen to persuade everyone to have a smart meter in place of their conventional meter. The marketing is focused on the possible energy savings and control over their energy use by using the data a smart meter will display.

However, there are privacy and security concerns that have not been publicised by the government or the energy companies. Smart meters record the total electricity consumption of a particular house. This is effectively an aggregated representation of all the different electrical appliances in the home.

Through your smart meter your power company (and government) can track things like how many people are typically home at certain times of the day and your family’s sleeping and eating schedules. They even know when a home is vacant, who has high-priced appliances, and who has a security system.

With smart meters, utilities typically collect thousands of times more data than required to calculate a monthly bill and thus expose residents to unnecessary risks. The Electronic Privacy Information Centre created this shocking list of possible dangers of smart meter data landing in the wrong hands:
“Identity theft, determine personal behaviour patterns, determine specific appliance used, performing real time surveillance’s, targeted home invasions, decisions and actions based upon inaccurate data, profiling, unwanted publicity and embarrassment, tracking behaviours of renters.”

German researchers Dario Carluccio and Stephan Brinkhaus said "Unfortunately, smart meters are able to become surveillance devices that monitor the behaviour of the customers leading to unprecedented invasions of consumer privacy,".

Energy law expert Chris Martin of Pinsent Masons said "The data can reveal much about a household, such as the make and model of their TV, the times during which a house is occupied and the number of people staying in a household.

This information is useful to energy suppliers, but it is also potentially valuable to a whole host of other organisations too,”.

Data Breaches

Smart energy meters collect and transmit detailed information about your energy usage, which could be valuable to cybercriminals. If a hacker gains access to your meter, they could steal your personal information, such as your name, address, and energy consumption patterns. They would know when the house was vacant and the best time to gain access to your home.

Hacking

Hackers could gain access to your smart energy meter and manipulate the data it collects, which could lead to inaccurate readings and higher bills. They could also use the meter as a gateway to the consumer's home network, enabling them to gain access to other devices connected to your network. An attacker who takes over the control facility or who takes over the meters directly could create widespread blackouts; a software bug could do the same.

Data Gathering and Theft

Smart energy meters use wireless communication to send data, which can be intercepted by unauthorized individuals, leading to the theft of sensitive information and system harm. Strong security measures are crucial to protect against data breaches and maintain privacy.

Privacy Protection Solutions

Numerous researchers have expressed their belief that existing privacy protection methods are either too expensive, too weak, or lead to an inefficient exchange of information. Another concern with smart energy meters, which are internet-connected and can be accessed remotely, is their vulnerability to hacking and cyberattacks. If an attacker gains access to a smart meter, they could tamper with the meter's readings or disrupt the energy flow in the grid. This could result in serious safety risks, as well as financial losses for both utilities and consumers.

Chris Oakley is vice president of technical services at the cybersecurity firm Nettitude. He says," Occasionally, smart meters have a glitch, resulting in customers receiving erroneous bills. These issues usually get sorted out quickly, but it demonstrates that these meters are vulnerable".

There have also been concerns that smart meters used to monitor gas supply could fail over the next few years as many are fitted with batteries that run out after about a decade. Unless batteries are replaced by an engineer, the smart meter could stop working, potentially shutting off the supply of gas.

Data Harvesting

In October 2022, the UK government confirmed that it would be using data from smart meters to get better insights into the rollout of the Energy Price Guarantee (EPG) scheme. However, experts suggest that this process could result in a breach of confidentiality and privacy.

Shadow Energy Minister Alan Whitehead said: "This proposal is an outrageous piece of private data-plundering and goes against every assurance put in place concerning the privacy of data generated from smart meter use”. “It needs to be stopped immediately. There are many other ways to check on possible fraud in obtaining EPG refunds.”

Nick Hunn, Founder of consultancy firm WiFore, commented: “Customers were promised their smart meter data would only ever be shared with their supplier. For the government to go back on this without a consultation sets a dangerous precedent.”

As a Privacy Advocate I’m continually asked by concerned people whether smart meters are safe, and would I recommend they have one installed. From my years of research, it is still apparent that there are many privacy and security concerns with smart meters for me to recommend having one installed.

Online privacy is dead! You cannot do anything to protect it!

This is what these organisations want you to believe. Mark Zuckerberg – CEO of Facebook said to Congress "**privacy was no longer a social norm**". This is from an organisation that makes billions in profit from manipulating and monetising its users.

The good news is that you can still use the Internet but in a safe and private way. You do not have to be manipulated and monetised. You and your family can have privacy online you only need to be shown how to do this.

As a Digital Privacy expert, let me show you how you can take simple steps to protect your privacy and personal safety and that of your family.

Your Digital Footprint

Your digital footprint is the amount of your data that is harvested and stored online. You need to take practical steps to reduce your digital footprint. The less data that can be harvested from you results in your social profile being worth less and less. The smaller your digital footprint the more privacy you and your family have. The more privacy you have the more you are a human being and not a commodity.

Cash is King

Every time you use any digital payment method (Google or Apple pay, credit or debit cards) your purchase is recorded, and that data is shared with a wide range of third parties. This is added to the vast amount of other data about you and the more data you share the more you are a valuable commodity.

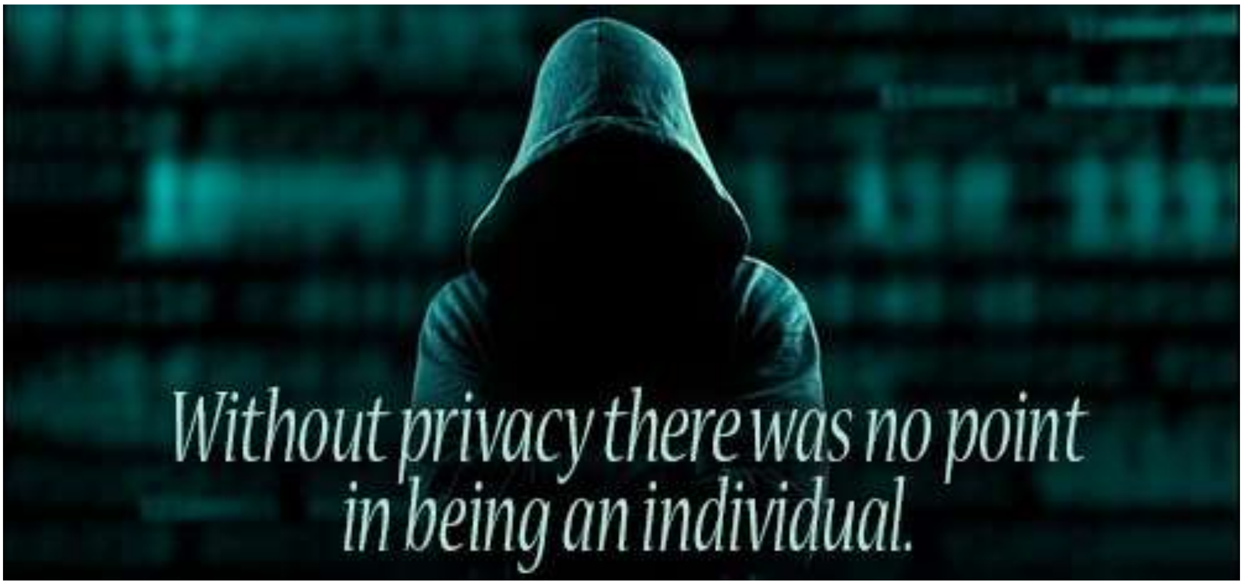
Cash is king when it comes to protecting your personal purchase data. Cash leaves virtually no trace. When buying with cash only the buyer and seller are aware of the transaction. what is bought, how much, when, where, by whom and at what price, all valuable information about an individual's habits.
It is easy for criminals to skim debit or credit cards and create copies of these cards. Using cash for payments protects you from card skimming scams. With cash there is no transaction fees, and you are not dependent on technology to work to undertake the purchase. Cash is a great way to take control of your finances and budget responsibly. It is easy to overspend using digital payment methods. Using cash will help you not go over your overdraft limit with the bank.

How private is social media?

As I have already stated Facebook is a toxic platform where their users have no privacy and they are just a commodity to control, manipulate and monetise.

Ideally it would be more beneficial if you could delete your Facebook account and associated apps and move over to a more private social media platform like Mastodon and Bluesky. I appreciate that this may be hard for some users to do as the platform is designed to be addictive as Facebook needs you to stay on the platform so it can continue to harvest your family's data to sell. I would therefore recommend removing all personal data from your profile and keep the information you share on this platform to a minimum. Everything you share on this platform is NOT private and is sold. Facebook app harvests data from your mobile even when you are not using it.

This also goes for Facebook Messenger, WhatsApp (owed by Facebook) and Instagram.



Is there a private alternative to WhatsApp or Instagram?

I come across many people who are unaware that WhatsApp is owed by Meta (Facebook). They assumed that WhatsApp is a private communication platform. This unfortunately is not the case. In 2014, when Facebook decided that it wanted to add WhatsApp to the 'Facebook Family,' the European Union (EU) only approved the deal after Facebook assured them that the two companies, and their data, would be kept separate.

It didn't take long for Facebook to go back on this agreement. In 2016, WhatsApp updated its Privacy Policy to allow sharing of data from WhatsApp to Facebook. Although they didn't reveal the full extent of this data transfer, it included your phone number and your usage data, like when you last used the service.

In January 2021, Facebook released a new data sharing policy for WhatsApp users in America, mandating the transfer of your information between the messaging app and social network. The information can include your profile photo, location, demographics, battery status, Wi-Fi-signals, users connected to the router, phone model, browser, time zone, and phone IMEI (unique identifier).

Besides that, WhatsApp would collect information that is believed to be more private. Such data includes how you are messaging, calling, and what groups are you part of, last seen, and much more.

Millions of WhatsApp users, concerned about the privacy aspect of this change by WhatsApp, moved over to using the privacy focused communication app called Signal.

One of the primary issues with WhatsApp is that it is owned by Facebook and suffers many of the same privacy dangers and misinformation campaigns as their parent company. Recently WhatsApp has been fined 225 million euros by the European Union (GDPR) for privacy violations. This is just one of many fines it has been given for serious invasions of user's privacy and data over the years.

Privacy alternative to WhatsApp

Signal is a private and secure messing service. It is so private that Mark Zuckerberg and his family uses it instead of WhatsApp. Signal has all the features that you will find in WhatsApp but is private. All your data, including metadata is not stored by signal servers. Both cryptography experts and privacy advocates recommend Signal. In fact, it is so private that it is recommended by Edward Snowden (Privacy Advocate).

I can personally recommend Signal as a privacy alternative to WhatsApp, and it is my main communication platform. Signal is privacy and security by design.

How do I encourage my family and friends to move to Signal?

Start a conversation about privacy with your family. You could let them read this, so they have a better understanding of why privacy is so important to protect. They can email me for further advice and to discuss why it would be beneficial to move to a privacy based secure messaging app like Signal. **The key thing here is that someone must make a stand and move to Signal**. Politely explain to your family and friends the reason why you have decided to leave WhatsApp. You will find that although it may take some time, most of your family and friends will eventually start to use Signal, especially if you are no longer using WhatsApp. Explain to your family and friends that they can install Signal and keep WhatsApp on their phones. I explained to my family and friends that their privacy and security was just as important to protect and using Signal rather than WhatsApp would give us all privacy and security. This approach worked and although it took some time, they did eventually all move to Signal. In the future they will be grateful that you took the decision and made the effort to improve the whole family's privacy and personal safety.

Is there a search engine that does not track you?

Google, Yahoo and Bing track all your searches, and this data is added to your social profile. Your search terms are very valuable to these tech organisations. The other issue with Google search is that it only shows you results that Google have been paid to show you. So, you do not see an un-biased view of the Internet just what Google has been paid to show you. This allows Google to control the feed of data to its users and control what they see and read and what they think is true. The power Google has on information control and the manipulation of its users is staggering.

How have we allowed one un-regulated data harvesting corporation to control the worlds information!

Think what it would be like if you could only buy one (government-controlled) newspaper or television channel to get all your news and information. You would only be fed biased information. This is exactly what you get when you use Google search.

Startpage is a privacy-based search engine that do not track you. Their results are **non-biased** and are not shared with any other organisation. You get a better range of website links than you would if you used Google search. To use Startpage just type this into a search engine and click on the link to be taken to the website. You can also type their website address – **startpage.com** into the address bar at the top of your browser and press the Enter key on the keyboard. Startpage offers better search results which are all kept private, why would you still use Google search?

What is a Honeypot

A honeypot is an online place where these data harvesting companies can access a large amount of data about a user. These honeypots are a lucrative money earner. Google, Yahoo and Microsoft Outlook (Live & Hotmail) free email accounts are the perfect honeypot as users store large amounts of your data that can be add to their social profile. There is no privacy if you use these email accounts. Your emails, calendar, contacts are all read, recorded, stored, and sold. The data harvested from these email accounts are very valuable to tech companies and data brokers. Would you be happy for everyone to read all your emails?

Is there a private alternative to data harvesting email accounts?

Proton mail is a free privacy-based email services that offer private encrypted email. It offers a free account and has the same features as the other non-private email account. The other bonus is that there is no advertising, so it is a more enjoyable experience, and the interface is so simple to use anyone can find their way around. I have been using Proton mail for a few years and I can highly recommend them to anyone who wants to use a privacy focused email account. They need **NO** personal information to set up an account. **Remember when you create your Proton email address do not use your full name as the email address.**

Proton have a useful wizard to help you migrate from your email provider to Proton Mail.

Proton is an open-source privacy focused organisation that has a range of privacy products including Proton Mail, Calendar, Drive, VPN & Pass.

Is there a private alternative to Google maps?

When you use Google maps your location is tracked, recorded, and sold. Google can track you and your family's location inside and outside, to a few metres. Just think about this, Google follows your family's every step. Would you be comfortable with a stranger following you around and then selling your location data? This location information is available to anyone who is willing to pay Google for access. The personal safety implications of this extremely accurate tracking are immense.

Also remember Google will share your location data with the police and other government agencies. Of course, Google's marketing makes it seem like this is all for your own good when in fact it is all about harvesting all your personal data for profit.

I would recommend turning off Location Tracking. This feature is found in the **Settings** menu of your phone. Search online for instructions on how to turn off Location tracking.

OsmAnd (osmand.net) is a more privacy-based mapping service. OsmAnd is a map and navigation app for Android and iOS. Map data can be stored on the device for offline use. Using the device's GPS capabilities, OsmAnd offers routing, with visual and voice guidance, for car, bike, and pedestrian. All the main functionalities work both online and offline. Maps can be downloaded to the device for use when there is no internet access. It has excellent privacy credentials as it is open source, and all the data produced is kept on the mobile not shared on the Internet.

On the desktop I recommend using Open Street Maps (openstreetmap.org).

Is there a private alternative to Chrome or IE (Edge) browsers?

When you use Google Chrome or Microsoft Edge (Internet Explorer) browsers to surf the web they track everything you do online. Chrome is happy to collect all your data through its browser and sell it to other third parties, essentially enabling a free-for-all when it comes to hugely sensitive information about your every activity, your every behaviour. Google Chrome browser is the most privacy destroying of any browser on the market today. As Google's business model is monetizing your users' information then their browser is the ideal way to access that data. Researchers have found that Google Chrome collects more data than any of the other browsers even if you are using their incognito mode. A browser does not need to collect every bit of a user's data to function.

Germany's Federal Office for Information Security says that Google's new browser Chrome "should not be used for surfing the Internet." The problem is that joined with email and search, Chrome gives Google too much data about its users.

Brave (brave.com) browser is more privacy based. Brave also has plugins that protect you from hidden Facebook and Google trackers that are on most websites. Search for Brave Browser in a search engine and download the browser (Brave app available for mobile phones). Then uninstall Google Chrome from your computer and internet devices including your smart phone. Brave browser has its own built in private search engine.

Compartmentalisation

Browser compartmentalization is a method of splitting your online activity into different browsers, so that whatever you search for in browser one isn't tracked in browser two. For instance, let's say you want to split your browsing activity into two: social media & email, and everyday browsing. Use one browser, like Mullvad, to sign into and access your email and social media accounts and another separate browser, like Brave, for any other type of browsing. Cookies can't share data between browsers, meaning your email and social media accounts can't track anything you do in the Brave browser.

For example, I use Brave browser for general web browsing and Firefox browser for accessing my email account and Mullvad for accessing my bank online.

How can I make my mobile phone more private?

Smart phones are the most successful privacy removing, surveillance device on planet Earth. Users put their whole life on their smart (surveillance) phone without any though of the privacy and safety implications of trusting Google or Apple.

If you use a phone that is not an iPhone (made by Apple) then it will probably have Google Android software installed by default. This is crazy that we have allowed Google to have the monopoly on over seventy percent of the mobile phones on the planet. Google has direct access to all the data on these phones. There is no privacy with Google Android operating systems.

When you use a Google Android phone, or a phone made by apple (iPhone) you must create an account and sign in to install any application (apps) and use the phone. This information and the phones unique identifier (IMEI) help Google and Apple to track your phone anywhere on the planet. Google and Apple dictate how you can use your phone and what apps are available for you to use.

The Washington Post conducted a privacy experiment to see how much personal data apps and other features of a smart phone gleaned from its user. The newspaper reported that 5,400 hidden app trackers sent data from a single phone.

Keep the number of apps you use to a minimum and use your browser (hopefully Brave) to access information instead of relying on apps. When you install apps, they can have hidden trackers in them to collect and share personal information on your phone with data brokers. For example, if I need to see what the weather is going to be for the week I would open Brave and type in “weather for Portsmouth” and Brave will show the weeks weather. No data harvesting and no weather app needed.

There are two options for making your mobile phone more private.

Option one:

For mobile privacy I recommend using an iPhone. Although Apple is not totally privacy based it makes most of its profit from selling its hardware not your data. It is easier to make the iPhone more private. I am not saying an iPhone is totally private just more private that a phone running Google Android software.

I appreciate that iPhones can be expensive to purchase so I would recommend buying a second-hand iPhone instead of a new one with a phone contract.

I can recommend the following company that sells second-hand iPhone: **theioutlet.com**. I have purchased my own iPhone from them as well as many for my clients. Excellent service and products.

Option two:

If you are interested in a near private and secure mobile phone, then I would recommend using GrapheneOS as your mobile operating system. Graphene started off as a mobile privacy project to make the world's most private mobile operating system.

GrapheneOS allows you to use a mobile phone without signing into any company, no Google or Apple sign in needed to install apps or use the phone.

A key security feature of GrapheneOS is its strict application sandboxing. Each app runs in its own isolated environment, preventing it from accessing sensitive data or interfering with other apps. This ensures that even if one app is compromised, the rest of your device remains secure.

GrapheneOS also includes a robust permission system that gives you full control over which apps can access specific features or data on your device. This allows you to fine-tune your privacy settings and ensure that only trusted apps have access to your personal information. Furthermore, GrapheneOS implements regular security updates to keep your device protected against the latest threats. These updates are delivered directly from the GrapheneOS team, ensuring that you receive timely patches and fixes to address any potential vulnerabilities.

In addition to its security features, GrapheneOS also prioritizes user privacy. It includes built-in privacy-enhancing technologies, such as support for hardware-backed keystores and secure disk encryption. This means that your data is encrypted and protected, even if your device falls into the wrong hands.

Another notable benefit of GrapheneOS is its commitment to transparency. As an open-source project, the entire source code is available for scrutiny, allowing security experts to identify and fix any potential vulnerabilities. This transparency ensures that GrapheneOS remains a trustworthy and secure operating system. Furthermore, GrapheneOS is designed with performance in mind. Despite its robust security features, it doesn't compromise on speed or usability. You can enjoy a smooth and responsive user experience while knowing that your device is protected. With F-Droid and Aurora app stores you have access to apps to install on your phone.

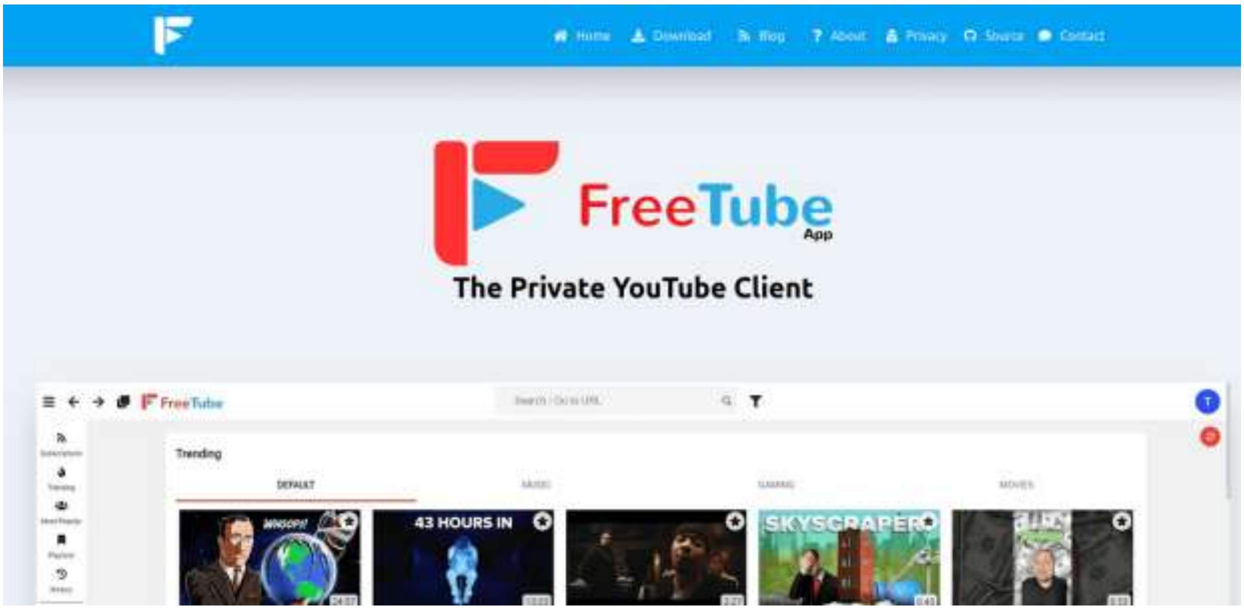
I have been using GrapheneOS on my phone for a while now and it is excellent at protecting your privacy and security. I now enjoy using my mobile phone as I have full control of my privacy and the permissions I give to apps. For a no obligation demonstration of GrapheneOS please feel free to contact me.

Is there a privacy alternative to YouTube?

As YouTube is a Google product is records and sells all the viewing information from you and your family. This data is added to your social profile. Your viewing habits on YouTube can inform Google so much about you and your family.

Odysee.com is a good alternative to YouTube. Although it currently does not have the same amount of content that YouTube has the content is growing each month and many Tubers have now moved their content to Odysee.com. Another advantage is that the adverts are not embedded into the videos. Odysee is a great privacy alternative to YouTube.

If you must use YouTube, then I recommend using Freetube (https://freetubeapp.io) which will allow you to watch YouTube videos through Freetube without any data harvesting from Google. Install Freetube on your computer and you can view YouTube video with no data tracking and adverts. On mobile phone use the app NewPipe.



Is there more information to keep my family private online?

If you would like more information on protecting your family’s online privacy, then check out my blog page on my website: **https://computerfixed.co.uk**

Please feel free to contact me if you would like to recommend a topic to be included in my privacy blog page.

I recommend checking these privacy knowledgeable bloggers on the platform Odysee.com.

- Techlore
- Naomi Brockwell
- Rob Braxman
- The Hated One
- Andy Yen (Proton CEO)

Recommended Digital Privacy books:

Shoshana Zuboff – **The Age of Surveillance Capitalism**. A useful book covering how your personal date is used to control, manipulate, and monetize you and everyone on this planet:

Michael Bazzell - **Extreme Privacy What It Takes to Disappear**. This book covers how to become more private online and offline:

James Bridle - **New Dark Age: Technology and the End of the Future**. A fascinating book that highlights the problems we are faced with the ever-expanding sea of data and information surrounding us.

Websites and Digital Privacy documentaries

A good source of privacy guides can be found at Privacy Guides website:

https://www.privacyguides.org

Privacy International aims to protect everyone's privacy:

https://privacyinternational.org

A digital privacy blog website:

https://computerfixed.co.uk/wp/category/online-privacy

Website for privacy software and apps:

https://www.privacytools.io

Proton blog on all things privacy:

https://proton.me/blog

Using Freetube (on desktop) or Newpipe (on mobile) search for the following documentaries:

- Glenn Greenwald: Why privacy matters
- Nothing to hide 2017
- The A.I. Dilemma - March 9, 2023
- The Social Dilemma 2020
- Google's The Selfish Ledger

Do we really want our children's future to be in a world where they are a commodity to be bought and sold? Where every aspect of their lives is recorded, stored and that personal data used to manipulate, discriminate, and control their behaviour and thinking.

Convenience using technology is great, but it comes at the expense of your and your family's privacy and safety. As an individual and a family, you need to decide how much convenience versus privacy and safety you are willing to have.

Ask yourself what is more important, privacy and personal safety or convenience!

As a Digital Privacy Advocate, I'm here to advise you on how to protect your family's privacy and safety so feel free to contact me.

"A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves, an unrecorded, unanalysed thought". Edward Snowden.

Use the Internet in a Safe and Private Way Course

This five-session course will introduce you to how to use the Internet in a safe and private way. With identify theft and online scams as well as data harvesting a major concern, it is important people know how to navigate the dangers on the internet and keep themselves safe and private.

Contact me for details of the dates the course will be running.

Listed below are the common proprietary software and the privacy alternative.

Proprietary Software	Privacy Focused Alternative
Adobe Illustrator	Inkscape
Adobe Photoshop	Darktable or Gimp
Apple or Google Podcast	AntennaPod
Edge, Chrome & Safari Browsers	Brave Browser
Facebook & Twitter	Mastodon
Google Authenticator app	Aegis Authenticator app
Google Maps	OsmAnd
Google Mobile Operating System	GrapheneOS
Google Play store	Aurora store & F Droid
Google search	Startpage (Startpage.com)
Google, Yahoo & Microsoft Mail	Tuta or Proton Mail
LastPass password vault	KeePassxc
Microsoft 365/Teams	Nextcloud
Microsoft Azure Virtual Machine	VirtualBox
Microsoft Bitlocker	VeraCrypt
Microsoft Media Player	VLC Player
Microsoft Office	Libre Office
Microsoft OneDrive	Nextcloud
Microsoft OneNote	Simplenote
Microsoft Outlook Desktop App	Thunderbird
Microsoft Windows 10 or 11	Linux Mint
NordVPN or Proprietary VPN’s	IVPN or Proton VPN
Plex	Jellyfin
WhatsApp & Skype	Signal
YouTube	Newpipe app or Piped on browser
Zoom	Calyx or Jitsi Meet

Listed below are a digital privacy checklist to aid your family on their digital privacy journey.

☐Move to Linux Mint operating system.
☐ Use multiple browsers (compartmentalisation).
☐ Implement tabbed browsing.
☐ Use a private search engine (Startpage.com).
☐ Use Alt + F4 to close popup windows.
☐ Use a password vault (Keepassxc or Proton Pass) to store all your passwords/passphrases.
☐ Regularly check Haveibeenpwd website to see if your email has been acquired in a data breach.
☐ Use an authenticator app (Aegis) or token (Yubikey) for MFA.
☐ Install and use a VPN on all Internet connected devices.
☐ Use cash on all purchases where possible.
☐ Changed the default network name and password on my router.
☐ Use open-source software instead of closed-source software.
☐ Use a privacy respecting email service (Tutamail or Protonmail).
☐ Use proxy emails instead of your original email address.
☐ Regularly keep updated on digital privacy news via websites.