Technology Has Changed the Face of Privacy. Here's What You Need to Do Next.

In the 21st century, privacy has become something of a political hot potato. The rich and powerful have been able to make use of 'super-injunctions' to protect their privacy, whilst unprecedented surveillance of the public has become normalised through CCTV and increased state powers.

However, privacy is supposed to be afforded to us all. Article 12 of the Universal Declaration of Human Rights says "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence", something also backed up by Article 8 of the Human Rights Convention here in the UK.

A Disruptive Digital Landscape

One of the biggest reasons behind recent challenges to our privacy is the rapid development and wide-reaching use of digital and web-based technologies.

In 2013, Edward Snowden showed the world the extent to which these digital footprints were used to surveil citizens across the globe by exposing how America was collecting the phone records of tens of millions of people. Ever since then, state and corporate surveillance has been in the spotlight, as our right to privacy has been eroded in multiple ways by a multitude of powerful stakeholders.

It's not just a matter for the UK either. In 2016, the Government implemented the Investigatory Powers Act, replacing a similar act which has since been found unlawful. Both bits of legislation have been heavily criticised for being far too wide-reaching in its data collection (meaning it wasn't targeted), as well as having a lack of independent oversight and the costs and scale of making it a reality.

However, all is not lost. Citizens still have the power to try to protect their online privacy. Indeed, knowing some of the ins-and-outs of surveillance has helped develop better and stronger technologies to combat it, as well as promoting best practice to a wider pool of users.

But knowing where to start can be tricky – there is no single model to protect your privacy, after all, we all have different priorities. Thankfully though, there is support for you on your journey to protect your right to privacy.

Creating an Honest and Full Risk Assesment

A crucial first step to increasing your digital security is to understand what data you are protecting, whom you are trying protecting it from, and the extent to which you are prepared to go in order to protect.

In the security and privacy business, this risk assessment process is often referred to by the rather militaristic phrase “threat modelling”. A great and very user-friendly guide to assessing your risks is available from the Electronic Frontier Foundation, as part of their Surveillance Self Defence guide. Your threat model will highlight the tools which are part of the route to enhancing your security.

Your behaviours and the way you use them are how you move forward and protect your privacy.

Another resource to help familiarise yourself with the context of digital surveillance is Tactical Tech Collective‘s My Shadow. This is a user-friendly website that contains a great breadth and depth to understanding how and why you can enhance your security and reclaim some privacy in your digital life. Amongst all of the information is a very useful eight-day Data Detox kit which can walk you through your first practical steps into enhancing your digital security.

Passwords: A Fundamental Building Block to Privacy

One of the foundational blocks to privacy is passwords and passphrases. Common guidance around passwords has led to an onslaught of weak passwords and worse practice.

Repeating passwords across a range of services, saving passwords in web browsers, and using logins made up of personal details are just some of the problems which making hacking your passwords easy.

The answer is to make passphrases longer and more random than your typical password. Tools such as diceware can help you to create more secure passphrases, but this comes with the complication of managing them, as they’re not something you’d likely remember (especially after a pint).

Thankfully, there are free and open source applications such as KeePassX to assist you in making your secure passwords usable!

Keeping Conversations Behind Closed Doors

Communicating online has become part of our daily lives, whether that’s through emails, messenger services or on social media. However, there are endless ways this can be tracked and used, something which can have a particularly chilling effect on freedom of speech.

To help protect yourself, and your rights, encryption tools can be used to scramble messages in transit, leaving only the sender and receivers able to decrypt and access the communications. There are a range of approaches for this across various platforms, and your risk assessment will help you to identify the right approaches for you.

One of the most highly regarded secure SMS, voice, and video call tools is the free and open source application Signal, which is built and maintained by the Open Whisper Group. The encryption protocol that Signal uses has been deployed in WhatsApp, but there are question marks around how the metadata is handled by WhatsApp’s parent company, Facebook.

Encrypting email is somewhat more complex, although the Free Software Foundation's email Self Defense is a comprehensive guide for configuring PGP encryption on your email. Other services such as Protonmail offer alternative forms of encryption and storage of email.

Web Browsing in Safety

Web browsing is another aspect of contemporary life which various corporate and state-level actors have active interests in. Again, the way we all use web browsers differs, but it is incredibly important to select web browsers that serve your needs.

If a web browser makes specific claims regarding its security, ask if the code is open-source, allowing security researchers to validate its claims. Browsers such as Mozilla's Firefox and Brave Browser are open source, whereas Microsoft's Edge, Apple's Safari, and Google's Chrome are all closed-source (although Chrome is built on the open-source Chromium).

Many browsers also allow extensions or add-ons to customise the browser. Sensible use of these can help you to enhance a browser's security. The extension HTTPS Everywhere, for example, is built by EFF and the Tor Project, and helps to force connections over the encrypted HTTPS protocol wherever it has been implemented by a website, giving users enhanced privacy.

The extension Privacy Badger is another great piece of technology built by EFF, and it helps to block invasive trackers such as third-party tracking cookies, often embedded within adverts that are presented on websites and used to track your web usage. Privacy Badger becomes more effective over time and allows users to have complete control over how it functions, rather than controlling the user's experience.

A Growing Suite of Privacy Protections

There are a wealth of more advanced strategies, tools, and processes available to further enhance your digital security and protect your right to privacy. From selecting secure VPNs to mask your IP address, to using the Tor Browser to add extra layers of protection to your identity, the more you investigate your privacy, the more you can do to increase it.

Companies, governments and other actors may be important players in the world of digital privacy, but ultimately it's our own behaviours and actions that will dictate our success in upholding our rights.

Becoming familiar with tools, how they work, and how you can make use of them is essential, and an ever-evolving process which directly affects us all.