Internet privacy

What is internet privacy?

Internet privacy or online privacy is the level of privacy protection an individual has while connected to the internet regarding their own data.

Privacy includes personally identifiable information such as the data that can be used to identify an individual. Alternatively, it includes non-personally identifiable information such as the websites visited by an individual or the behaviour on individual websites.

I have nothing to hide – why should I care about internet privacy?

Privacy is a fundamental right. Edward Snowden remarked "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

As doctors we all work in the public domain and have to be identified as medical doctors when using social media platforms in a medical capacity. This also means that we can be identified online by our patients through platforms like the General Medical Council. Additionally, we can all be searched for through search engines, and any personal pictures can even be used to geolocate where we are at any particular time through social media platforms. Whilst we may exist in small or large social media communities, the internet connects us with millions of individuals who may have grossly opposing views or agendas. Privacy of personal information will be increasingly important.

How am I being tracked across the internet?

Cookies are small pieces of data stored by internet browsers as you visit a website. First party cookies store data related to visiting that site only. Third party cookies store data relating to you visiting multiple other websites.

Third party cookies can encourage other technologies such as 'fingerprinting' which essentially force your browser to give up technical data about your computer, your browser and your screen resolution. By combining multiple pieces of information, a fingerprint unique to you is formed and can allow targeted adverts directly to you. Even using private browsing modes and virtual private networks (VPNs) may not prevent fingerprinting as those connections themselves form part of the fingerprint.

What can you do to improve your online privacy?

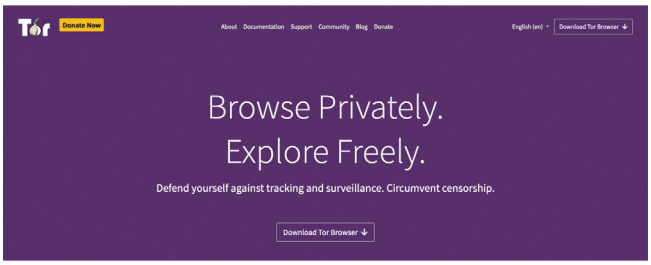
There are a variety of different techniques you can use to improve your online privacy and security.

For security, turning on fingerprint identification on your mobile phone, and signing websites using two factor authentication are easy ways to improve access to your personal information. Internet browsers can also store passwords securely which should mean the end of easy to guess passwords for a multitude of websites.

Internet browsers

Tor Browser (Mac, Windows, Linux) – Provides the highest level of internet privacy by routing your browsing through several encrypted layers. However, it is much slower than traditional browsers and provides flawed search engine results in reviews.

Mozilla Firefox (Mac, Windows, Linux) – A wide variety of security and privacy features in a fast browser. Privacy modes include private browsing, tracking protection and ad blockers.



Google itself is developing a ***Privacy Sandbox*** (available to try in Chrome – Settings / Privacy and Security / Privacy Sandbox). The Privacy Sandbox is currently in testing (beta) in certain countries. The aim is to prevent the tracking of individuals but still allow tailored advertising. Controversially, this would put Google at the centre of the control of an individual's online privacy whilst other websites would not have the same degree of control.

Microsoft Edge and ***Safari*** have also made moves to give a more private internet browsing experience.

Browser extensions

DuckDuckGo (Chrome, Microsoft Edge, Firefox, Opera) – This browser extension can be installed and then defaults to DuckDuckGo as the search engine and offers privacy blocking of trackers.

Privacy Badger (Chrome, Microsoft Edge, Firefox, Opera) – This browser extension stops advertisers and third-party trackers from secretly tracking where you go and the pages you look at on the web.

Ghostery (Chrome, Firefox, Microsoft Edge, Opera) – A privacy extension which blocks ads, protect your privacy by blocking trackers.

Apps

Jumbo Privacy and Security (iOS and Android) – helps with locking down security settings through multiple platforms including Facebook, Google, Twitter and Amazon. The downside is that maximum protection costs £7.58 per month.

DuckDuckGo Privacy Browser – Unlike conventional search engines (Google, Yahoo, Bing), DuckDuckGo is a search engine which focuses on user privacy. It attempts to stop the collection of cookies and blocks targeted ads. The search options are not as wide as the major search engines and the privacy blocking is not complete given the large number of ways user privacy can be exploited on the internet.

SECTION EDITOR

Ivo Dukic,
Consultant Urological Surgeon, University Hospitals Birmingham Foundation Trust.
E: ivodukic@gmail.com