Founding Partner
OPTUS

MACQUARIE University

Online Browser Privacy

DR JOHN SELBY

CONTENTS

INTRODUCTION

Whilst the Internet's many benefits for individuals, businesses and society have been obvious over the last twenty-five years, it has taken longer for some of its harms to be recognised and understood. Recent revelations about tracking by governments (Snowden leaks) and businesses (Facebook/Cambridge Analytica) and "Fake News" have led many people to express concern about risks the Internet has introduced into their lives. This Whitepaper identifies some of those risks and argues that taking steps which improve your online browser privacy may be one way to increase the net benefits both you and society experience from the Internet.

WHAT IS ONLINE BROWSER PRIVACY?

The privacy paradox [29] is a concern that whilst people say they want privacy, their actual behaviour suggests that they don't really care about their privacy enough to actually protect it. One reason for this is that the average person is so busy living their day to day life that they remain rationally ignorant of many of the relatively easy things they could do to improve their privacy. This Whitepaper seeks to encourage greater online browser privacy as a way to help address one aspect of the privacy paradox.

Online Browser Privacy is the idea that an Internet user should be empowered to more easily and effectively decide what and how much personal and technical information they wish to disclose about themselves and their computer whilst using the Internet. Achieving this empowerment requires: 1) awareness and understanding of the risks of online browsing; and 2) taking action to install and use tools which can make it relatively simple to achieve your desired level of online browser privacy.

WHY IS ONLINE BROWSER PRIVACY IMPORTANT?

Whilst many different protocols and technologies constitute the Internet, the most popular tool through which billions of Internet users access a wide variety of online information each day (whether on their computers, tablets or mobile phones) is through their Internet browser software (such as Mozilla Firefox, Google's Chrome, Microsoft Edge/Internet Explorer, Apple's Safari, etc.).

When visiting websites through their Internet browser (whether to watch videos, search for information using a search engine, read an online newspaper, or doing their internet banking), there is communication in two directions between that internet browser and the servers hosting that information. Just as you can click on a link to request Youtube's server to send you a video file of a kitten playing a piano, Youtube's server can ask your computer to send it some (or a lot of) information. Many internet companies' business models are based upon this exchange: those companies provide Internet users with access to free information/services in return for information about the internet user which the company can sell to advertisers (summed up in the aphorism: "if you are not paying for something online, you are the product"). This exchange becomes more complex when those internet companies cross-reference information your browser has disclosed to one (or hundreds) of websites to build up a detailed profile about you which they can exploit for profit.
Whilst some Internet users might find value in that exchange of free information/services for their personal information, this is not without risk. Two such risks include:

1) the disclosure of personal information about the Internet user whilst browsing ("***Tracking Risks***"); and
2) the use of that collected personal information to display of advertisements on the Internet user's browser ("***Display Risks***").

TRACKING RISKS

There are four main risks for Internet users who disclose personal information through their browser which permit them to be tracked: the first is from online advertisers, the second is from online merchants, the third is from search engines, and the fourth is by your Internet Service Provider/Government Agencies/Law Enforcement. Each of these risks is discussed below.

Tracking by advertisers:

The tracking of Internet users is desired by Internet advertisers as it enables them to more efficiently select and target audiences for their advertisements as compared to broadcasting advertisements to more general audiences through the traditional advertising mediums of television, radio or print. Thus, if an advertiser believes that a particular demographic group is more likely to respond to their product or service offering (whether through a click-through or a "like"), then they will seek to serve their advertisements to only those Internet users who fall into that demographic group. Whilst traditional demographic groupings, such as gender, age, etc. have been a feature of traditional advertising mediums, the Internet provides advertisers with a level of demographic granularity far greater than what can be achieved through advertising via traditional mediums.

The first risk posed by the tracking of Internet users is that it permits online advertisers to discriminate against certain people by biasing the audiences to which those advertisements are shown. Examples have been seen of bias that arguably could amount to discrimination within online advertisements, such as not showing higher-paying job advertisements to Internet users identified as women, the aged, or minorities [12] [33]; hiding apartment rentals from certain racial groups [4] [5], or stereotyping criminality by delivering advertisements about bail-bond services to African-Americans [41].

If an Internet user is not supplying personal information to online advertisers, then those advertisers will not be able to (as) easily identify the demographic group into which they wish to classify that Internet user. This would ensure that the Internet user was able to receive (if they so choose) advertisements targeted at a wider range of demographics than otherwise would be the case. The practical implication of this is that the Internet user who better protected their online privacy may be more likely to see an advertisement for a higher-paying job or a better apartment than would be the case if advertisers could determine more easily that the Internet user fell into a category whom the advertiser wished to exclude from receiving its advertisements. The downside is that a user may see more irrelevant advertisements (but this is something which can be resolved by blocking all advertisements as discussed below).

Tracking by Website Operators:

Unlike a traditional supermarket which typically offers to sell each product at the same price for all customers, operators of online stores reveal their price for a good or a service separately to each customer. This means that they can practice what is known as "price discrimination", which is charging higher prices for the same item to Internet users who they perceive may be willing to pay more than the price that item is offered to other Internet users. Price discrimination in itself may not be illegal, but over time it can be quite expensive for an Internet user to be easily identified as a member of a group who the retailer believes should pay more than others. In order to more efficiently increase their profits, the website operator desires to know information not only about how each Internet user interacts with that operator's website, but also to know information about what other websites the Internet user has visited and information about the user themselves. For example, some websites have charged higher prices to Internet users who visited their online stores using particular web-browsers because those merchants believed that (for example) people who purchased Apple products were more status-conscious, and were not as budget-conscious as the average Windows or Linux-user [35]. In other reported examples, Newegg charged 40% more for a television to users of the Firefox or Internet Explorer browsers than it did for users of the Chrome browser and Walmart.com charged Firefox browser users 15% more for a laptop than it did for users of the Chrome and Internet explorer browsers [11].

Tracking by Search Engines

At first glance, it might seem paradoxical that search engines (such as Google or Bing) are both free services *and* the basis of enormously valuable (>AUD1 Trillion in 2018) businesses [55]. The reason why search engines are regarded as immensely valuable businesses is because they enable their operator to collect an extraordinarily-detailed insight into Internet users which can be analysed and sold to advertisers. Search engines lower the transaction costs [37] associated with finding information online, whether it is "what airline should I take to fly from Sydney to Beijing?" or "what types of mortgages are available"? The questions that Internet users ask evidence their wants, needs and desires, and can often be of such an intimate nature that most people would otherwise not ask them of a friend or neighbour.

Whilst any one single search query might only reveal a small amount of information, aggregating all of the searches done by an Internet user over a period of months or years can reveal to a search engine operator an incredibly detailed portrait of that person's wants, needs and desires. Advertisers are (collectively) willing to pay billions of dollars per year to companies like Google, Facebook or Microsoft to deliver advertisements targeted towards Internet users who have searched for particular keywords. Search engine operators host millions of auctions per second to find the advertiser willing to pay the most money to them for the right to

deliver an advertisement which will be displayed to you along with the results of the search you have just made [53].

The information that search engines know about you can be used in a variety of ways which might harm you. First, the search engine can use that information about your past searches to make inferences (assumptions) about you which skew the results it delivers to you when you conduct a new search for a different topic. Second, the search engine can voluntarily (or by the compulsion of court orders such as subpoenas, or through secret National Security Letters), pass on your search history to third parties including civil litigants, law enforcement and intelligence agencies. Those entities can then use that information to act in a variety of ways which might be harmful to you.

Tracking by Internet Service Providers, Government Agencies and Law Enforcement

Typically, between you (as an Internet user) and the websites you wish to visit sits an Internet Service Provider (ISP) who charges you a monthly subscription fee to access the Internet. If you are using free Wi-Fi at a coffee shop or airport lounge, the shop-owner or lounge operator is paying the Internet Service Provider a monthly subscription fee to provide you with that service.

ISPs can potentially know more about your online browsing habits than search engines [26]. This is because for every website you visit or link you click on it is typically the case that your computer will first ask your ISP for information about the Internet Protocol address (a numerical address roughly equivalent to a phone number) for the server which hosts that domain name (known as a DNS query). For example, if you type into your Internet browser ‹www.mq.edu.au› to visit Macquarie University's website, your computer will first query your ISP to find out the IP address before it uses that information to request information from the Macquarie University webserver to display within your Internet browser. An ISP can keep a record of each DNS query you make, thus building up a pattern of your Internet browsing habits. If the ISP uses a technology known as Deep-Packet Inspection [21], it is possible they can know not only with whom you are communicating online but also what you are saying.

Whilst some Internet users might say "I have nothing to hide and nothing to fear" from my ISP, that does not apply to all Internet users, nor at all times, nor in all countries. It is also ignorant of historical events, some of which were revealed by Edward Snowden [3]. Some ISPs have given access to their customers' data streams (whether voluntarily or by legal mandate) to government agencies and law enforcement, which has resulted in mass surveillance, the erosion of civil liberties and, in some cases, arrests, torture and incarceration [21]. For example, since April 2017 Australia's Mandatory Data Retention laws [47] have compelled Internet Service Providers to retain two years of metadata about Internet users' online activities and to provide access to that retained metadata to an ever-growing (rarely disclosed) list of local, state and federal government departments and law enforcement agencies [10]. The intelligence leaks by Edward Snowden in 2013 revealed that the Five Eyes intelligence agencies had used programs known as PRISM and UPSTREAM to gain bulk access to online communications [49].

DISPLAY RISKS

Permitting online advertisements to be displayed on your computer poses at least three risks. The first relates to harms against your computer; the second relates to manipulation of Internet users through those advertisements in ways which can pose harm to democratic institutions; the third relates to the expense associated with the bandwidth required to display advertisements.

Fake News

An even more significant risk from online advertisements is the threat to democracy from "Fake News" advertisements. Scholars have already shown that viewing online advertising can influence political decision-making, particularly amongst the least-educated, who may not have had the opportunity to develop sufficient critical thinking skills which could inoculate them against that "fake news" [32]. Instances of this include the 'weaponised advertisements' used by (amongst others) Russian intelligence agencies in attempts to conduct information warfare to manipulate voters by showing them fake news via targeted online advertisements during (amongst others) the 2016 U.S. Presidential election [28] [51] [52] and the Brexit referendum in the United Kingdom [27].

Malware-vertising

We have seen that some online advertisements have been used to deliver malware (for example, advertisements presented recently on Microsoft's Edge browser to Internet users who searched on Bing.com for "Google Chrome" have led those users to fake websites from which mal-ware laden versions of Google's Chrome browser would be downloaded [19]. Those advertisements were used by criminals as a vehicle through which they could achieve their end goal of committing financial crimes, such as stealing from Internet users' bank accounts, etc [36].

Bandwidth costs of advertisements

The third risk is not one experienced by all Internet users – it tends to fall upon those who live at the geographical margins of our societies. Whilst city-dwellers may not notice the bandwidth consumed by online advertisements, Internet users in regional and remote areas who rely upon satellite Internet connections might prefer to reduce their monthly Internet bills by avoiding excess download charges resulting from downloading online advertisements. More recently, this risk has diminished somewhat in Australia as the National Broadband Network has included satellite internet services in its offerings [54]. However, it is still a risk for Internet users in remote areas of other countries.

HOW CAN GREATER ONLINE BROWSER PRIVACY BE ACHIEVED?

Your online browser privacy can be improved by installing a number of software tools designed to protect your privacy against different types of threats. Each of these is discussed below. However, before going into the details, it is worth briefly mentioning two strategies which have (unfortunately) failed to deliver on its promises of improving your online browser privacy: DoNotTrack and PrivateBrowsingMode/IncognitoMode.

THE FAILURE OF DO-NOT-TRACK TO PROTECT ONLINE BROWSER PRIVACY

After consumer groups advocated for several years to the U.S. Federal Trade Commission [2] for better privacy protection, when it was first launched in 2010-11 as a function within Microsoft's Internet Explorer and Mozilla's Firefox browsers, the Do-Not-Track tool inserted a header (DNT:1) into information sent by those browsers to web servers which indicated that the website's operator should not track the user. Unfortunately, this was an unenforceable request to the website operator who was free to ignore it. Major U.S online advertising groups such as the Digital Advertising Alliance, the Council of Better Business Bureaus and the Direct Marketing Association did not require their members to honour the requests to "Do-Not-Track" and there was no legal recourse available to an Internet user whose requests were ignored [34]. Whilst it proved relatively popular amongst Internet users, unfortunately, by 2018 it was apparent that the Do-Not-Track setting within browsers was recognised and implemented by only a tiny fraction of websites and that the operators of almost all of the most popular websites ignored it and tracked their Internet users [25]. Any online browser privacy that Internet users might have hoped for by using Do-Not-Track had become illusory and it had failed as a self-regulatory solution.

WHY IS PRIVATE BROWSING MODE/INCOGNITO MODE INSUFFICIENT TO COMPLETELY PROTECT YOU?

A relatively recent innovation by Internet browser software developers (such as Mozilla Firefox, Google Chrome, Apple's Safari and Microsoft Edge) has been to introduce an option which reduces the traces that your browsing of the Internet leaves on your own computer. Unfortunately, whilst these options offer some improvement to your online browser privacy, they are not complete solutions. Notably, the threats those options protect against relate primarily to people who might be able to gain physical access to the electronic device through which you have been browsing the Internet (whether on a PC, laptop, tablet, smart phone, etc.). Leaving fewer tracks of your online browsing habits might be useful to protect against snooping by your employer, spouse, parent, or a customs agent whilst you are crossing a border. However, these options do not protect against the tracking risks and display risks (discussed above) caused by leakage of information about your online browsing habits to third parties such as Internet Service Providers, advertisers, site operators, search engines, etc. Therefore, further effort is required to improve your online browser privacy.

TOOLS WHICH CURRENTLY WORK TO ENHANCE YOUR ONLINE BROWSER PRIVACY

Below are four categories of tools which can help you to enhance your online browser privacy. Unfortunately, advertisers, website operators and others have a strong incentive to try to undermine your online browser privacy by constantly dreaming up new techniques to track Internet users, so the actual effectiveness of these tools can vary over time as their developers take time to identify those new techniques and to develop effective counter-measures. Consequently, these tools are unlikely to provide you with complete online browser privacy forever – these tools will need to be updated and/or replaced over time as new threats emerge.

TOOLS TO PROTECT AGAINST REVEALING PERSONAL INFORMATION TO YOUR ISP

The first tool which may help reduce tracking of your online browsing by your ISP is a Virtual Private Network (VPN). When properly configured, this is a service which limits the information known to your ISP to only the fact that you have made an encrypted connection to one external server (which is operated by the VPN company. All of your internet browsing would then be routed via the VPN company's server(s). This results in a slight slow-down of your internet service which may affect the quality of time-sensitive online activities, such as Internet-gaming, video calls, streaming services, etc. Indeed, the New Zealander Kim Dot-Com only realised he was under surveillance by U.S. government agencies when he noticed a significant slow-down in the performance of a computer game he was playing (due to those agencies re-routing all of his internet traffic via their U.S. servers to conduct surveillance upon him) – those agencies had effectively installed a surveillance VPN without Dot-Com's permission [18].

Whilst there are many VPN services advertised on the Internet, not all of them are equal. Typically, free VPN services are not worthwhile, indeed some can be dangerous [24] [45] [56]. Depending upon where you live, what you do online, and who you think might desire to surveil and/or possibly cause you harm, different VPN services might be more, or less, appropriate. Alas, a thorough analysis of the best VPN providers is beyond the scope of this Whitepaper (and any such recommendation would rapidly become out-dated). Fortunately, there are a number of VPN testing and review services which are semi-regularly updated that can help you to decide which (if any) VPN may be best for your specific needs [44] [46] [48].

The second tool which can help protect your privacy against your ISP is to not use their DNS servers to lookup the IP addresses of websites you wish to visit. Fortunately, there are alternatives (such as OpenDNS [9] – though it is now owned by Cisco which may present its own risks to some users) and it is not compatible with some VPN services (which should provide their own DNS lookup servers).

TOOLS TO PROTECT AGAINST REVEALING PERSONAL INFORMATION TO SEARCH ENGINE OPERATORS

Whilst search engines such as Google and Bing are very popular, there are ways to conduct searches on those sites without revealing your personal information. For example, three ways to get results from Google's search engine whilst protecting your privacy are to search using Startpage [40], DuckDuckGo [14] or DisconnectSearch [13]. These are all proxy search engines (the first two do the search on Google for you and Google only knows that Startpage/DuckDuckGo have done thousands of searches, not who the individual Internet users were who actually requested the search results). Disconnect delivers results from multiple search engines, including Google, Bing and Yahoo [43].

TOOLS TO PROTECT AGAINST REVEALING PERSONAL INFORMATION TO WEBSITE OPERATORS

As discussed earlier, many website operators have a strong motivation to want to gather as much information about Internet users as possible and to track their online browsing from one website to the next. Some researchers have identified at least 85 different techniques which website operators can utilise to extract and identify individual Internet users and to extract personal information from their browsers [20]. A combination of the tools listed below installed and properly configured into v63 of the Mozilla Firefox browser on the author's computer managed to block all of those different privacy-invasive techniques in October 2018. Of course, new privacy-invasive techniques emerge every day, so not all Internet users will achieve the same result over time [57], [58].

There are (at least) fourteen tools which you can install into your internet browser to limit the information that you disclose whilst visiting websites online. No single tool offers complete protection on its own, so Internet users are encouraged to select the combination of them which best suits their needs. Each of these is discussed below, generally in alphabetical order (except for the first tool which works best if it is installed before the other tools). To avoid the risk of malware, each of these tools should only be installed using the browser's internal capability to install add-ons/plug-ins, etc. For a useful guide on how to install tools such as these into the most popular Internet browsers, see: Computer Hope, 'How to Add Extensions to Your Browser' ‹https://www.computerhope.com/issues/ch001888.htm›.

First: a few disclaimers. Some of these tools may be harder to configure than others. Some may break certain websites (e.g. cause a blank page to load instead of the information you want to see) until you adjust your settings, others may be detected by the website operator and result in them asking you (politely or not-so-politely) to turn them off before they will serve you all of their information. Some (such as NoScript) will often require you to take a small number of additional steps to load webpages using only the javascript that you want to permit whilst prohibiting third-party javascripts to run. In a corporate environment, some computers may be locked-down so that you lack the authorisation to install these tools (if so, ask your IT Department nicely and they might install them for you). These tools will not protect you against malware or ransomware already installed on your computer. These tools are not a replacement for a properly configured firewall and anti-virus software. Some of these tools may collect limited anonymised information from your computer in their default modes [59]. If you are using a computer provided to you by your employer (or another person), they may still be able to surveil your internet browsing even after you install these tools. I, and the Optus-Macquarie Cybersecurity Hub, are not providing any technical support for these tools and are not liable for any harm you suffer if you install them.

i. Disconnect

Disconnect enables you to visualise and block a variety of techniques through which websites seek to track you. Due to its relative ease-of-use, Disconnect was named the best privacy tool by the New York Times in 2016 [8]. However, it only accurately counts the number of tracking tools it blocks if it is installed before the other privacy protecting tools listed below. It works on Firefox, Chrome, Safari and Microsoft Edge (and on your mobile phone).

ii. AdBlock Plus

AdBlock Plus interrogates the code sent to your computer by each webserver and identifies which components are requests to load advertisements into your browser. It then simply discards that information so that your browser only shows you the useful information on the requested webpage (without showing you the advertisements). It also blocks tracking, malware domains and social media buttons from loading. By default, it will permit some ads to load, but you can easily change its configuration settings to un-tick that box (which I recommend you do). It works on Firefox, Chrome, Safari and Microsoft Edge (and on your mobile phone).

iii. Behind the Overlay

Behind the Overlay is a tool which can be used to counteract steps taken by some website operators to restrict your access to their webpages due to your installation of other privacy-protecting tools (notably AdBlock Plus). It is helpful when the website operator uses javascript to raise a partial barrier (like a curtain) to your reading all of the information on their webpage (known as an Overlay). Behind the Overlay allows you (in most situations) to click one button to remove that partial barrier. It works in Chrome and Firefox.

iv. Clear Flash Cookies

Whilst cookies were originally invented to enable online stores to keep track of what items you had added to your shopping cart, those cookies have since been used to facilitate tracking of Internet users. More complex versions, known as "Super Cookies", also exist. Both can track you even after you close down your Internet

browser and re-open it. This tool will automatically delete both cookies and Super Cookies each time you re-open your Internet browser. It works in Firefox.

v. Firefox Multi-Account Containers

This tool allows you to create virtual browsers within Firefox, so that you can log into the same website using different accounts at the same time. This enables you to risk-assess your browsing and keep separate your work email from your personal email, your work search history from your personal search history, your work social media account from your personal social media account, and your work banking/investments from your personal banking/investments. It works in Firefox.

vi. Facebook Container

Similar to the Firefox Multi-Account Container listed above, this is a narrower tool which isolates your Facebook usage from being tracked by third parties and Facebook from tracking your usage of third party websites. It does not protect against Facebook collecting, using or disclosing information that you post on Facebook. It works in Firefox.

vii. Firefox Lightbeam

Rather than explicitly blocking third-party tracking of your Internet usage, Lightbeam visually displays to you what tracking is present on a particular webpage and how the operators of those tracking tools are able to link your activity across different websites. It was first presented (at the time Lightbeam was called "Collusion") at a TED Talk in 2012 [30]. It works only in Firefox.

viii. GHOSTERY

Ghostery is a tool which allows you to manually select which third-party tracking techniques you wish to block [22]. It blocks nothing by default (but you can select to block everything with a few mouse-clicks in its configuration settings). For greater privacy protection, you might want to configure Ghostery's own settings so that you untick the "Opt-in" tracking options which send some information back to Ghostery. It works in Firefox, Chrome, Safari and Edge browsers, plus on Android and IOS devices.

ix. https Everywhere

Https Everywhere [15] is a tool developed by the Electronic Frontiers Foundation in the USA. It automates the use of the Secure Hypertext Transfer Protocol (https://www.xyz.com) rather than using the original (insecure) Hypertext Transfer Protocol (http://www.xyz.com). Effectively, it saves you from having to remember to type in the extra 's' each time, so provides greater privacy by default. It works on the Firefox, Chrome and Opera browsers.

x. NoScript

Endorsed by Edward Snowden, NoScript [38] is a tool which, by default, blocks Javascript, Flash, Java and certain other privacy-invading plug-ins from loading when you open a web-page. It protects against cross-site scripting attacks, cross-zone DNS re-binding, CSRF (router hacking), and clickjacking attacks. You can determine which (if any) scripts you wish to permit to run on a webpage. NoScript is a very powerful privacy-protecting tool, but it can result in quite a few blank webpages until you permit (temporarily allow) certain of the scripts from those pages to run. Some Internet users may find it too much of a nuisance for daily usage, but those who desire higher levels of privacy whilst online browsing are encouraged to at least try it. It only works in the Firefox browser.

xi.  Privacy Badger

Privacy Badger is another tool developed by the Electronic Frontiers Foundation [16]. It is designed to detect when different (third-party) sources are attempting to track you across multiple websites. Rather than coming with a default block list, Privacy Badger attempts to learn from your browsing habits. If it detects such tracking, it then prevents your browser from loading any more content from that source. This includes attempts at what is known as 'canvas fingerprinting' which is a technique by which website operators try to uniquely identify you from the various settings you have configured in your browser. It works in Firefox, Chrome and Opera browsers.

xii.  Random User-Agent

Random User-Agent is a tool designed to prevent tracking through browser fingerprinting. Browser fingerprinting is a method of uniquely identifying Internet users by synthesising a range of 17 specific settings their Internet browser reveals to a web server each time it requests a webpage [31]. It is relatively easy to find out how unique your particular browser (and its settings) are [1]. Disclosure of these settings was originally designed to enable website operators to deliver information to your screen in a format which was best-suited for it (imagine trying to look at the same information on your mobile phone screen as that which would be best suited for a desktop-user with a 30" monitor). However, website operators and advertisers have realised that the myriad of various settings that people use can result in each Internet user being uniquely identifiable – as uniquely identifiable as a human fingerprint.

The only way to counteract this ability to track an Internet user across every website they visit is to deliver randomised fake information about your browser settings to each website you visit. Random User-Agent permits you to do this easily. The only downside of using this tool is that sometimes websites will deliver to you incorrect information based upon this fake information (e.g. delivering an update for a software program designed to be installed onto an Apple Mac rather than a Windows PC, or not letting you update a browser add-on to the latest version because the website believes you are using an out-of-date browser. Fortunately, Random User-Agent can be turned off for specific websites (or globally to resolve temporary issues). Just remember to turn Random User-Agent back on after you have resolved any such issues which emerge. It works in Firefox and Chrome browsers.

xiii.  Social Disconnect Plus

Social media website operators (such as Facebook, Twitter and Linkedin) have encouraged third party website operators to add "like buttons" to those third-party websites. Whilst those buttons might permit Internet users to more easily demonstrate their interest in particular third-party content to their friends on social media, such functionality also enables those social media website operators to track internet users as they browse across the Internet (even if they have not clicked on the "like button" on a particular webpage) [39]. Social Disconnect Plus detects and blocks the loading of social media "like buttons". It works in Firefox.

xiv.  uBlock Origin

uBlock Origin is a tool designed to block ads, trackers and malware sites [50]. It is similar in functionality to AdBlock Plus, though it claims to be more efficient. It works in Firefox, Chrome, Safari and Microsoft Edge browsers.

TOOLS WHICH CAN PROTECT YOU AFTER YOU HAVE FINISHED BROWSING THE INTERNET

One final step which can help reduce the risk that any of the above tools might have failed to detect a new method of tracking your online browsing activities is to use a software cleaning tool each time after you have finished browsing the Internet/just before you disconnect from a VPN/each time you close down your computer. Such tools are designed to securely delete (i.e. over-write multiple times) the contents of certain locations on your hard disk which might contain information that could be used to track your online browsing activities/computer usage. One popular tool is "CCleaner" [7], though a recent version (5.45) of it was criticised for lacking certain privacy protections (since patched). CCleaner is currently free for home use, but business users would have to pay a licence fee to use it. An open-source free alternative is "BleachBit" [8]. Caution should be taken when configuring either Bleachbit or CCleaner to ensure that you do not accidentally configure it to delete critically

important personal or work files (such as your photos, reports, etc.) or files necessary for the proper functioning of your operating system/installed programs.

CONCLUSION

This Whitepaper has explored a variety of ways in which a range of stakeholders can threaten your online privacy. It identified six main interest groups who may desire to interfere with your privacy: online advertisers, online merchants, search engine operators, criminals, government agencies (including law enforcement and intelligence agencies) and Internet Service Providers. It identified how threats to online browsing privacy may emerge from both the collection of your personal information and the display of advertisements and other bits of information (such as social media "like buttons") on webpages you request. It then provided information on privacy-friendly search engines, browser plugins and software which you might install and configure to minimise the harms which could flow from those threats. You are encouraged to explore the extent to which these tools (and others) are best suited to address your own particular needs whilst browsing online.

ABOUT THE AUTHOR

Dr John Selby is an academic in the Faculty of Business and Economics at Macquarie University and a member of the Optus-Macquarie University Cybersecurity Hub. His interdisciplinary research focuses on the spill-over effects of the Internet on business, including cybersecurity, privacy, AI and distributed ledger technologies. Dr Selby can be contacted at: john.selby@mq.edu.au

BIBLIOGRAPHY

1. Am I Unique https://amiunique.org/fp
2. Julia Anwin and Jennifer Valentino-DeVries, 'FTC Backs Do-Not-Track System for Web' *The Wall Street Journal* (2 December 2010) [Online]. Available: https://www.wsj.com/articles/SB10001424052748704594804575648670826747094
3. Julia Angwin, et al, 'NSA Spying Relies on AT&T's 'Extreme Willingness to Help", *New York Times and ProPublica* (15 August 2015) [Online]. Available: https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help
4. Julia Angwin, Ariana Tobin & Madeleine Varner, 'Facebook (Still) Letting Housing Advertisers Exclude Users by Race' *ProPublica* (21 November 2017) [Online]. Available: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin
5. Charles Bagli, 'Facebook Vowed to End Discriminatory Housing Ads. Suit Says It Didn't.' *New York Times* (27 March 2018) [Online]. Available: https://www.nytimes.com/2018/03/27/nyregion/facebook-housing-ads-discrimination-lawsuit.html
6. Bleachbit: https://www.bleachbit.org
7. CCleaner: https://www.ccleaner.com
8. Brian Chen and Natasha Singer, 'Free Tools to Keep Those Creepy Online Ads From Watching You' *New York Times* (17 February 2016) [Online]. Available: https://www.nytimes.com/2016/02/18/technology/personaltech/free-tools-to-keep-those-creepy-online-ads-from-watching-you.html
9. Cisco, *OpenDNS* https://www.opendns.com/setupguide
10. Melissa Clarke, 'Metadata Laws under fire as 'authority creep' has more agencies accessing your personal information' *ABC News* (19 October 2018) [Online]. Available: https://www.abc.net.au/news/2018-10-19/authority-creep-has-more-agencies-accessing-your-metadata/10398348

11. Stephanie Clifford, 'Keeping an Eye on Bouncing Prices Online' *New York Times* (27 January 2013) [Online]/. Available: https://www.nytimes.com/2013/01/28/business/new-online-price-trackers-alert-shoppers-to-good-deals.html
12. Amit Datta, et al, 'Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice and Discrimination' (2015) 1 *Proceedings on Privacy Enhancing Technologies* 92-112
13. Disconnect Search: https://search.disconnect.me/
14. DuckDuckGo: https://www.duckduckgo.com
15. Electronic Frontiers Foundation, *HTTPS Everywhere* https://www.eff.org/https-everywhere
16. Electronic Frontiers Foundation, *Privacy Badger* https://www.eff.org/privacybadger
17. Electronic Frontiers Foundation, *Upstream vs PRISM* https://www.eff.org/pages/upstream-prism
18. David Fisher, 'Suspicion Over Dotcom Net Glitch' *New Zealand Herald* (5 October 2012) [Online]. Available: https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10838484
19. Mary Jo Foley, 'Microsoft Removes Fake Bing Ad That Looked Like a Chrome Download Site' *ZDNet (*28 October 2018) [Online]. Available: https://www.zdnet.com/article/microsoft-removes-fake-bing-ad-that-looked-like-a-chrome-download-site/
20. Gertjan Franken, Tom Van Goethem and Wouter Joosen, 'Who Left Open the Cookie Jar? A Comprehensive Evluation of Third-Party Cookie Policies' *Paper presented at 27th USENIX Security Symposium* Baltimore, USA (15-17 August 2018) [Online]. Available: https://wholeftopenthecookiejar.eu/static/tpc-paper.pdf
21. Christian Fuchs, 'Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance' (2013) 16(8) *Information, Communication & Society* 1328-1359
22. Ghostery: https://www.ghostery.com/
23. Laura Hautala, 'NSA Surveillance Programs Live On, In Case You Hadn't Noticed', *C/NET* (19 January 2018) [Online]. Available: https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/
24. Amelia Heathman, 'Android VPN App Developers Are Using Malware to Track Your Data' *Wired* (26 January 2017) [Online]. Available: https://www.wired.co.uk/article/android-vpn-apps-malware
25. Kashmir Hill, "Do Not Track,' The Privacy Tool Used by Millions of People, Doesn't Do Anything' *Gizmodo* (16 October 2018) [Online]. Available: https://www.gizmodo.com.au/2018/10/do-not-track-the-privacy-tool-used-by-millions-of-people-doesnt-do-anything/
26. Jacob Hoffman-Andrews, 'Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls' *Electronic Frontiers Foundation* (3 November 2014) [Online]. Available: https://www.eff.org/deeplinks/2014/11/verizon-x-uidh
27. Information Commissioner's Office, *Monetary Penalty Notice against Facebook Ireland Ltd and Facebook Inc* (24 October 2018) [Online]. Available: https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf
28. Kathleen Hall Jamieson, (2018) *Cyber-war: How Russian Hackers and Trolls Helped Elect a President: What We Don't Can't and Do Know*, Oxford University Press
29. Spiros Kokolakis, 'Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox' (2017) 64 *Computers & Security* 122-134
30. Gary Kovacs, 'Tracking our Online Trackers' (3 May 2012) [Online]. Available: https://www.ted.com/talks/gary_kovacs_tracking_the_trackers?language=en
31. Pierre Laperdrix, Walter Rudametkin and Benoit Baudry, 'Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints' *Paper presented to the 37th IEEE Symposium on Security and Privacy* (May 2016, San Jose, USA) [Online]. Available: https://hal.inria.fr/hal-01285470/file/beauty-sp16.pdf
32. Federica Liberini, et al, 'Politics in the Facebook Era: Evidence form the 2016 President Elections' (2018) *The University of Warwick Centre for Competitive Advantage in the Global Economy Working Paper Series, Paper No. 389* [Online]. Available: https://warwick.ac.uk/fac/soc/economics/research/centres/cage/manage/publications/389-redoano.pdf
33. Sarah March, 'Campaigners Begin Action Against Male-Targeted Job Ads on Facebook' *The Guardian* (19 September 2018) [Online]. Available: https://www.theguardian.com/technology/2018/sep/18/facebook-sued-gender-bias-male-targeted-job-ads

34. Lou Mastria, 'Digital Advertising Alliance Gives Guidance to Marketers for Microsoft IE10 'Do Not Track' Default Settings' *About Ads Blog* (9 October 2012) [Online]. Available: http://www.aboutads.info/blog/digital-advertising-alliance-gives-guidance-marketers-microsoft-ie10-%E2%80%98do-not-track%E2%80%99-default-set
35. Dana Mattioli, 'On Orbitz, Max Users Steered to Pricier Hotels' *Wall Street Journal* (23 August 2012) [Online]. Available: https://www.wsj.com/articles/SB10001424052702304458604577488822667325882
36. Annelies Moens, 'How to Lower Your Risk of Data Breaches at Home or at Work' *Legalwise* (5 July 2018) [Online]. Available: http://legalwise.com.au/news/lower-your-risk-of-data-breaches/
37. Douglass North, 'Transaction Costs, Institutions and Economic History' (1984) 140(1) *Journal of Institutional and Theoretical Economics* 7-17
38. NoScript: https://noscript.net/
39. Franziska Roesner, 'Detecting and Defending Against Third-Party Tracking on the Web' *Presentation to the 9th Usenix Conference on Networked Systems Design and Implementation* (26 April 2012, San Jose, USA) [Online]. Available: https://www.usenix.org/sites/default/files/conference/protected-files/nsdi-webtracking.pdf
40. Startpage: https://www.startpage.com
41. Latanya Sweeney, 'Discrimination in Online Ad Delivery' (2013) 56(5) *Communications of the Association for Computing Machinery* 44-54 [Online]. Available: http://dataprivacylab.org/projects/onlineads/1071-1.pdf
42. Josh Taylor, 'Telstra Logs Customer History for New Filter' *ZDNet* (26 June 2012) [Online]. Available: https://www.zdnet.com/article/telstra-logs-customer-history-for-new-filter/
43. Sven Taylor, 'Best Private Search Engines for 2018' *Restore Privacy* [Online]. Available: https://restoreprivacy.com/private-search-engine/
44. Sven Taylor, 'Best VPN Service Report' *Restore Privacy* [Online]. Available: https://restoreprivacy.com/best-vpn/
45. Sven Taylor, 'VPN Warning List – Is Your VPN Safe?' *Restore Privacy* [Online]. Available: https://www.restoreprivacy.com/vpn-warning-list
46. TechRadar, 'The Best VPN Service in October 2018' [Online]. Available: https://www.techradar.com/au/vpn/best-vpn
47. *Telecommunications (Interception and Access) Amendment (Data Retention) Act* (Cth) 2015
48. That One Privacy Site, 'Detailed VPN Comparison Chart' [Online]. Available: https://thatoneprivacysite.net/vpn-comparison-chart/
49. Craig Timbert and Ellen Nakashima, 'Agreements With Private Companies Protect U.S. Access to Cables' Data for Surveillance' *The Washington Post* (6 July 2013) [Online]. Available: https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html
50. uBlock Origin: https://github.com/gorhill/uBlock#ublock-origin
51. *United States of America v Internet Research Agency LLC and others*, (2018) Case 1:18-cr-00032-DLF (16 February 2018)
52. *United States of America v Elena Alekseevna Khosyaynova* (2018) Case 1:18-MJ464 (28 September 2018)
53. Hal Varian, 'Online Ad Auctions' (2009) 99(2) *American Economic Review: Papers & Proceedings* 430-434
54. WhistleOut, 'Editor's Pick: Best Satellite NBN Plans October 2018' [Online]. Available: https://www.whistleout.com.au/Broadband/Guides/best-satellitle-nbn-plans
55. *Yahoo Finance:* https://finance.yahoo.com/quote/GOOG/ and https://finance.yahoo.com/quote/MSFT/
56. Muhammad Ikram, et al, 'An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps' (2016) *Proceedings of the 2016 Internet Measurement Conference* 349-364
57. Imane Fouad, et al, 'Tracking the Pixels: Detecting Web Trackers via Analyzing Invisible Pixels' *Paper submitted to Arxiv on 4 December 2018* [Online]. Available: https://arxiv.org/abs/1812.01514

58. Muhammad Ahmad Bashir and Christo Wilson, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem' (2018) 4 *Proceedings on Privacy Enhancing Technologies* 85-103

59. Nullsweep, 'How to Detect if a Browser Plugin is Spying on You - A Complete Guide' (22 January 2019) [Online]. Available: https://nullsweep.com/how-to-detect-if-a-browser-plugin-is-spying-on-you/

Founding Partner
OPTUS

MACQUARIE University

OPTUS MACQUARIE UNIVERSITY

Cyber Security Hub

CRICOS Provider 00002J

This white paper is part of an insight and knowledge-sharing series from the Optus Macquarie University Cyber Security Hub.

The Cyber Security Hub relies on a network of experts across business, government and higher education. It promotes an interdisciplinary understanding of cyber security by bringing together technology, business, legal, policy, security intelligence and psychology perspectives.

The Cyber Security Hub offers a range of services and collaborative opportunities. This includes professional education, hosting events to promote up-to-date knowledge, publishing key insights and updates, and working with partners on their business challenges.

If your organisation would benefit from being a part of a cross-sector network and have a greater understanding of the complex issues surrounding cyber security, please contact us to discuss opportunities for collaboration at **cybersecurityhub@mq.edu.au**

For more information visit **mq.edu.au/cyber-security-hub**