Object-oriented Information Systems Blog Post: User Privacy Online

In many parts of the world, computing and the internet form a core part of everyday life. In Great Britain 96% of households had access to the internet as of February 2020 (Office of National Statistics, 2020). With the proliferation of internet connected personal devices such as smart phones and tablets, and the increasingly common use of Internet of Things devices such as smart speakers, this has opened the door to increased user tracking. This was brought into the eye of the general public when the General Data Protection Regulation (GDRP) was brought into effect in the European Union in May 2018. Since users are becoming more aware of the data they share online, whether purposefully or inadvertently, many are beginning to seek out ways of staying anonymous online.

One only has to listen to a podcast or watch a youtube video now to see or hear an advertisement for a virtual private network (VPN) service. A VPN is a service that allows its users to route their internet traffic securely through one of their servers located in various countries around the world. This allows users to browse securely open public networks in places such as cafes, and also obscures the sites that you visit from your internet service provider (ISP), and also obscures your location from the sites you visit by hiding your IP address (Kaspersky, N.D). The usage of VPN services is increasing every year. As of January 2020, 41% of U.S. and U.K. adults used a VPN service at least once a week, with 36% saying they used one almost every day (Miltz, 2021). There is no doubt that a percentage of these users will be using a VPN service to try to stay anonymous online, but with one of the primary advertising strategies of many VPN providers being to promote the ability to access region locked content on services such as Netfilx while using their service, it is not unreasonable to assume that many of the users connect to VPNs mainly for this purpose rather than privacy alone. While VPNs are a good and easily

accessible first step for many users, they do not completely prevent more advanced user tracking methods which are becoming more common today.

Browser fingerprinting is a method of identifying a user across multiple visits to a site, and across multiple websites via the collection of a variety data such as the user's browser version and window size, active plugins, screen size and resolution, and operating system. Any one of these pieces of information can seem fairly arbitrary, but when enough data points are combined it has been found that only 1 in 286,777 browsers will share an identical fingerprint (Hauk, 2021). This is a powerful tracking method employed by various advertisers to serve targeted ads to users, a practice that many people find "creepy" or unsavoury. Some modern browsers, such as the Safari browser included in macOS, hinder tracking via fingerprinting by presenting a simplified system information to trackers so that many devices look identical (Apple, 2019). In addition to this, Google is planning to remove the use of all third-party cookies from its Chrome browser by the end of 2022 in favour of implementing its own first party tracking solution as part of its "Privacy Sandbox". Google proposes to replace third party tracking in Chrome with an AI powered system which will place users into different groups based on their web history and other factors. Advertisers will them be able to serve ads to the one or more of the groups, while the specific user data used by Google for grouping will remain obfuscated. As Chrome is the web browser with the largest market share, this would significantly alter the way user data is collected and used for the better (Burgess, 2021).

As users continue to become more aware of web tracking and the privacy concerns that come with it, the demand for new solutions that maintain the users' anonymity while allowing websites to continue to be supported by advertising revenue will continue to grow.

This demand, along with new regulations such as GDPR, will necessarily encourage new research and development into how privacy can be maintained online.

References

Office of National Statistics. (2020) Internet Access - households and individuals, Great Britain: 2020. Available from: **https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2020** [Accessed 16 April 2021].

Kaspersky. (N.D) What is VPN? How It Works, Types of VPN. Available from: **https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn** [Accessed 16 April 2021].

Miltz, K. (2021) How often do you use a VPN? Available from: **https://www.statista.com/statistics/1219770/virtual-private-network-use-frequency-us-uk/** [Accessed 16 April 2021].

Hauk, C. (2021) Browser Fingerprinting: What Is It And What Should You Do About It? Available from: **https://pixelprivacy.com/resources/browser-fingerprinting/** [Accessed 16 April 2021].

Apple. (2019) Safari Privacy Overview. Available from: **https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf** [Accessed 16 April 2021].

Burgess, M. (February 2, 2021) Google's next big Chrome update will rewrite the rules of the web. *Wired.* Available from: **https://www.wired.co.uk/article/google-chrome-cookies-third-party-ads** [Accessed 16 April 2021].