# PRIVACY IN THE EU AND US:

## Consumer experiences across three global platforms

TACD Trans Atlantic Consumer Dialogue

HEINRICH BÖLL STIFTUNG BRUSSELS European Union

## Acknowledgements

**About the principal Author**
Pat Walshe is currently an independent consultant and founder of Privacy Matters. He has over 20 years of experience in the field of data protection and privacy. He is a passionate advocate for privacy and tweets from @privacymatters.

A special thanks also goes to Anna Fielder and Alexandra Graziano from the Transatlantic Consumer Dialogue (TACD) secretariat for coordinating and editing the report, to Finn Myrstad and Burcu Kilic, the TACD digital policy committee chairs, and to those on the advisory panel, all of whom worked hard to realise this report.

Finally, to those involved in the mystery shopping and subject access request exercise:

Mystery shoppers (in alphabetical order):
- Alexandra Graziano
- Deepika Yadav
- Maira Sutton
- Pat Walshe
- Zora Siebert

Subject access request (in alphabetical order):
- Anna Fielder
- Burcu Kilic
- Christoph Mayer
- David Martin
- Deepika Yadav
- Deborah Rodriguez
- Linda Sherry
- Pat Walshe
- Peter Maybarduk
- Upasna Bahl
- Zora Siebert

This report *Privacy in the EU and US: Consumer experiences across three global platforms* is jointly published by Heinrich-Böll-Stiftung Brussels European Union and the Transatlantic Consumer Dialogue (TACD), London, England.



This report is based on a review of company practices and information referred to in the report between September to October 2019.

The Transatlantic Consumer Dialogue has benefited from funding under an activity grant from the European Union's Partnership Instrument under the programme "EU-U.S.: Transatlantic Civil Society Dialogues (TCSD). While TACD receives EU grant support, this report was done outside that grant. The contents of this document are the sole responsibility of TACD and the Heinrich-Böll-Stiftung Brussels European Union and can under no circumstances be regarded as reflecting the position of the European Union.

# CONTENTS

# FOREWORD FROM THE HEINRICH-BÖLL-STIFTUNG BRUSSELS EUROPEAN UNION

Data protection is about safeguarding people and their privacy. For many, the focus is on protecting information, but it is actually about protecting people and ensuring that they remain in control.

Algorithms handling large volumes of data and the connectedness of our lives bring new threats to our autonomy. Europe answered this challenge with a comprehensive privacy reform that protects citizens' information from being a commodity for tech companies.

The General Data Protection Regulation (GDPR), which entered into force in May 2018, strengthened the protection of personal data for hundreds of millions of people in the EU and beyond. It lays out explicit rules on collecting, storing, sharing and using personal data, placing the burden of responsibility on businesses, not individuals.

GDPR is advancing the global conversation about data protection. Argentina, Brazil, Japan and India are overhauling and implementing their own privacy laws. In Washington, D.C., Congress is debating a comprehensive federal privacy law. California has already passed the California Consumer Privacy Act, which will enter into force on 1 January 2020. GDPR is a game-changer.

The Heinrich-Böll-Stiftung Brussels European Union strongly supports the development of local and international frameworks for personal data protection.

This is why our EU arm has partnered with the Transatlantic Consumer Dialogue to examine how three global platforms – Amazon, Netflix and Spotify – protect data on both sides of the Atlantic.

Pat Walshe's report reveals that the different standards have produced two classes of customers. In the EU, companies must inform customers of cookies and allow them access to the data these companies hold on them. Netflix and Spotify have extended this right to their US customers, showing how GDPR is changing global realities.

But it also highlights the persisting gap between law and practice, even in the EU. Reviews of the three companies' privacy policies and the experiences of "mystery shoppers" who set up accounts in the EU and the US show that the companies failed to inform consumers about their rights and options in clear language. Privacy policies should not require 20 minutes to read and a college degree to comprehend. And pre-ticked boxes do not amount to informed and active consent to being tracked by advertisers.

The report provides further evidence to support high standards of privacy and data protection throughout the US – not just California. For the EU, the lesson is that robust enforcement mechanisms are vital. This is the only path towards a global Internet regulation that treats privacy rights as what they are, namely fundamental human rights.

Eva van de Rakt
Head of Office
Heinrich-Böll-Stiftung Brussels European Union

HEINRICH BÖLL STIFTUNG
BRUSSELS
European Union

# FOREWORD FROM THE TRANSATLANTIC CONSUMER DIALOGUE

While the most revolutionary innovation of our time – the Internet – transformed our lives and our society, it has also created new challenges. With consumers increasingly relying on the Internet for work, education, shopping and social life, it is more important than ever that the appropriate regulatory frameworks are in place to ensure their privacy, safety and well-being.

Since its establishment in 1998 as an official platform for EU and US consumer organisations, the Transatlantic Consumer Dialogue (TACD) has promoted and advocated for consumer rights and protections in the digital world. TACD has the status of a consultative forum to the EU and US governments on issues relating to transatlantic consumer policy and contributes to the policy making process by ensuring key consumer priorities are regarded within EU-US regulatory and governmental processes.

TACD's EU members played a major part in the development of the General Data Protection Regulation (GDPR) by conducting a multi-year advocacy campaign and analysis effort around the legislative process in the European Parliament. The GDPR has led the way as the most comprehensive, consumer-centric privacy regulation of the Internet Age.

On the other side of the Atlantic, the US has no comprehensive privacy legislation comparable to the GDPR. The regulatory void has left US consumers at the mercy of online platforms, who have little incentive to safeguard personal data.

This report provides a broad context for better understanding of consumer privacy challenges across the Atlantic. It explicitly demonstrates that relying on companies to do the best for their customers voluntarily is not always enough. The importance of privacy rights and safeguards has never been more relevant than it is today. This report is a compelling call to regulators to take bold steps to legislate and enforce the rules that safeguard consumer privacy and security.

As TACD, we believe that strong privacy standards should apply to everyone who uses online platforms and services no matter where they live. We envision a digital economy that safeguards individual privacy, advances fairness and provides equal opportunity for all.

In Europe, the GDPR was only the start of the fight for data protection and we now need European regulators to enforce the law and provide further guidance, and consumer and privacy groups to investigate business practices and hold companies to account. In the US, it is time for Congress to enact a comprehensive and meaningful federal privacy law and provide a consistent set of rights, protections and practices.

Our hope is that the findings of this report will inspire thought and action in the US and EU. In the meantime, as TACD, we will continue to advocate for consumer rights and protections, identify possible legislative and regulatory solutions and a way forward by tapping into synergies and action from both sides of the Atlantic.

Dr. Burcu Kilic
TACD Digital Policy Committee
US Chair

Finn Myrstad
TACD Digital Policy Committee
EU Chair

Trans Atlantic Consumer Dialogue

## GLOSSARY OF TERMS

**Access volunteer** – individuals who submitted subject access requests for this research
**CCPA** – California Consumer Privacy Act
**CNIL** – Commission nationale de l'informatique et des libertés
**EDPB** – European Data Protection Board
**EU** – European Union
**ePD** – ePrivacy Directive
**FTC** – Federal Trade Commission
**GDPR** – General Data Protection Regulation
**Mystery shoppers** – individuals who, for this research, created accounts for each platform and captured relevant information related to the data protection and privacy notices and practices of the three companies
**NGO** – Non-Governmental Organisation
**TACD** – Transatlantic Consumer Dialogue
**UK** – United Kingdom
**US** – United States

# EXECUTIVE SUMMARY

Data protection and privacy laws are being introduced or reviewed around the world in an effort to keep pace with technologies and strengthen the protection of personal data and privacy online. It is important to look at how these regulations are being implemented and whether they help consumers exercise their privacy and data protection rights. But how consistent are consumers' experiences across different markets?

This research examines how aspects of privacy and data protection are working for consumers in two major economic areas – the EU and the US. Both have high levels of digital use, and major online providers offer very similar services in both regions. However, their legal approach to data protection and privacy are very different: while the EU has a general data protection law, the US to-date has not enacted such an all-encompassing law at the federal level.

Three major services providers, Amazon, Netflix and Spotify, were selected to examine to what extent their customers based in the US receive a standard of privacy and data protection comparable to that of their EU customers. This was done through a mixture of mystery shopping, requests for access to personal data made by volunteers, and an analysis of existing EU and US legislation including the General Data Protection Regulation (GDPR) and the e-Privacy Directive (ePD) in the EU, and the California Consumer Privacy Act (CCPA) in the US, which at the time of analysis and publication of this report, has not yet entered into force.

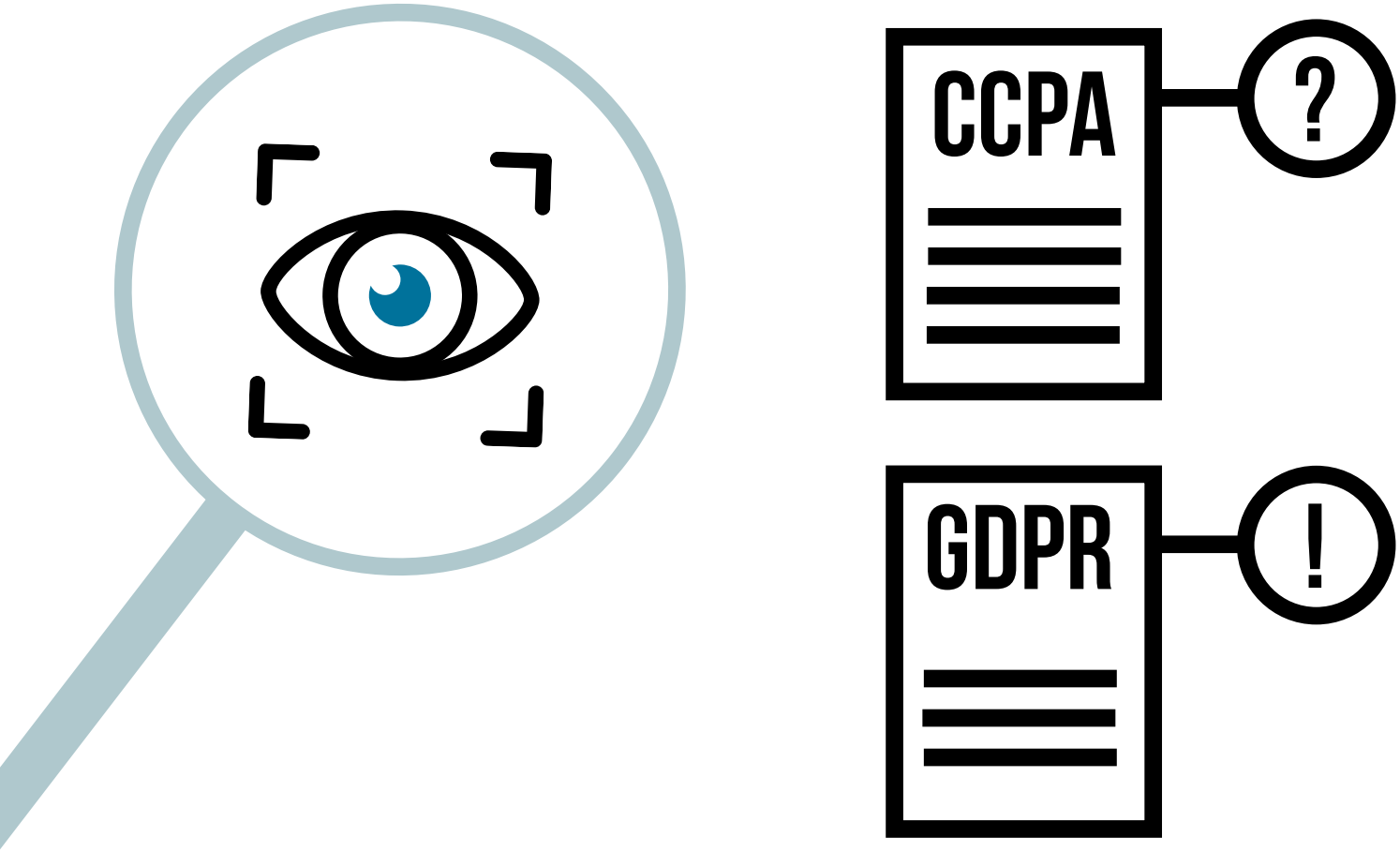
Based on the research carried out, the key findings reveal that:

- **Users cannot avoid being tracked.** All three companies use cookies and other means to track users by default for behavioural targeted advertising purposes. While Amazon EU, Netflix EU and Spotify EU do present cookie notices to visitors on their websites, they rely on implied consent that is contrary to the legal requirement of opt-in consent in the EU. The US counterparts of the three companies do not notify their customers of 'cookie' trackers altogether.
- **Third parties track users**. Each service appears to allow third-party tracking by default on their websites, with Amazon being the most and Netflix being the least intrusive of the three. This results in tracking of user behaviour and targeted ads.
- **Privacy policies and other related policies are generally hard to read**. They were found to be long, not concise or easy to understand.
- **Companies fail to provide proper transparency.** Even when operating under GDPR, none of the three companies clearly notify users of the specific purpose and legal basis for processing their data or how long it will be stored (retention).
- **Dark patterns appear to be present.** The use of design features and wording do not necessarily act in the interest of individuals nor appear to incorporate 'data protection by design' into their approach. These companies may set privacy intrusive defaults such as a pre-ticked 'tailored ads' option or use in-app tracking[1] for advertising purposes, neither of which are clearly notified to individuals.
- **Amazon treats US users differently in terms of rights to access.** Unlike Netflix US and Spotify US, the research discovered that Amazon US does not provide the same level of transparency nor gives its customers the 'right of access' to their personal data enjoyed by the EU customers of Amazon. Netflix and Spotify do not appear to treat their US customers differently from EU customers in these regards.

1. A review of the Android mobile apps for Amazon US/UK and Spotify US/UK found software code embedded for the purposes of advertising-related tracking and targeting. The Netflix Android app did not appear to contain such code.

The research findings on the specific topics analysed, question whether the companies are fully meeting their obligations on transparency, data protection by design and default, consent and key rights under the GDPR and the ePD. The findings also provide lessons relevant to the implementation and enforcement of the CCPA, as per regulations proposed by the California Attorney General. The proposed CCPA regulations are intended to *"establish procedures to facilitate consumers' new rights under the CCPA and provide guidance to businesses for how to comply."*

The findings show that key objectives of EU law, to ensure businesses are transparent and clear about their use of peoples' data and that they meet and make it easy to exercise key rights, requires stronger oversight and enforcement of legal protections. Consumer and privacy organisations can help enforcement by continuing investigations and taking cases to court as necessary. The findings also indicate that in the US, a baseline federal data protection and privacy law should be established that does not pre-empt stronger state law and protections and that creates an independent data protection agency. We give more detailed recommendations under each section of this report.



# 1. INTRODUCTION

In this report we assess the way in which three selected companies, Amazon, Netflix and Spotify, comply with key aspects of the European Union's (EU) General Data Protection Regulation[2] (GDPR), as well as the EU ePrivacy Directive (ePD),[3] that sets out additional rules about online tracking[4] of individuals based in the EU. We also examine to what extent US customers of these major service providers receive a comparable standard of data protection and privacy to their EU customers.

Amazon, Netflix and Spotify were chosen for this research as they offer equivalent services that are popular with consumers in the US and EU.[5] The practices of these companies provide a good opportunity to understand how they have implemented key aspects of the GDPR approximately 18 months after it took effect. The observations made during the investigation also help identify policy implications and lessons for future lawmaking and enforcement.

While the US has not yet enacted a comprehensive national data protection law, there is now growing interest in doing so following the introduction of the California Consumer Privacy Act of 2018 (CCPA)[6] which is due to come into force in 2020. While the GDPR is broader than the CCPA and based on a fundamental right to data protection,[7] both give customers the right to know what personal data is being processed, and obtain a copy of their personal data[8], and both provide a right to request deletion of this data in certain circumstances.

The report is based on an assessment of:

- How these companies meet key aspects of their obligation to ensure they are **transparent** about their collection and use of people's personal data;
- Whether the companies rely on **consent** and if so, if they meet the standard of consent set out in the GDPR;
- The companies' use of key **defaults** and settings that may impact on an individual's privacy;
- Whether they **share** individuals' personal data with third parties;
- The degree to which the companies are meeting their obligations with regards to an individual's **right of access**[9] to their personal data, including:
    - how transparent the companies are about this right
    - how easy it is to exercise
    - whether the companies demand proof of identity
    - whether the companies provide all the data people are entitled to; and
- The degree to which the companies are meeting their obligations on **data retention,** such as setting out the period for which data will be stored.

2. European Commission 'EU Data Protection Rules' www.ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#library and Regulation (EU) 2016/679 (the 'General Data Protection Regulation') www.eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

3. The ePD compliments the GDPR and seeks to protect the privacy and confidentiality of peoples' communications including their online activity. The ePD is sometimes known as the 'cookie law', though it is much more than this. It requires an organisation to obtain a user's consent before it stores or accesses information on a user's device, especially for cookies that track online browsing behaviour for example.

4. Article 5(3) of the ePrivacy Directive 2002/58EC as amended by Directive 2009/136EC www.eur-lex.europa.eu/legal-content/EN/TXT/ELI/?eliuri=eli:dir:2009:136:oj requires consent for cookies that are not strictly necessary such as ad-related cookies and pursuant to the EU Court of Justice ruling on 1 October 2019 www.curia.europa.eu/juris/liste.jsf?num=C-673/17

5. Amazon Around the World, Emarketer, 13/11/2018 www.emarketer.com/content/amazon-around-the-world. Number of Netflix paying streaming subscribers worldwide from 3rd quarter 2011 to 3rd quarter 2019, Statista, 18/10/2019 www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subscribers-worldwide/ Spotify website, www.newsroom.spotify.com/company-info/

6. CCPA www.oag.ca.gov/privacy/ccpa

7. Article 8, EU Charter of Fundamental Rights www.fra.europa.eu/en/charterpedia/article/8-protection-personal-data

8. The GDPR regulates the use of 'personal data', while the CCPA applies to 'personal information'. This report uses the term 'personal data' for consistency

9. The right of access is similar under the GDPR and the CCPA

The assessment also considered the use of any **dark patterns**.[10] A dark pattern may include design features that can *"trick people into doing things that they might not want to do but which benefit the business in question"*[11] on a website or app;[12] or that may obscure or hide from plain view important information and privacy intrusive defaults or that may otherwise make it difficult for people to discover and change defaults that can impact their privacy; or to find information about their rights and how to exercise them easily.

In the US, such practices may violate Section 5 of the Federal Trade Commission (FTC) Act,[13] and many state consumer protection laws. In the EU, in response to concerns over the use of dark patterns online, the French data protection authority (the CNIL) issued a report that made operational and policy recommendations to move from 'dark patterns' to data protection by design and user empowerment, as required by the GDPR.[14]

10. Mathur et al, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 2019 www.webtransparency.cs.princeton.edu/dark-patterns/sch et al, Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, 2016 www.petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf
11. Norwegian Consumer Council, Deceived by Design, 2018 www.fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf and Youtube website, www.youtube.com/watch?v=kxkrdLI6e6M
12. Dark Patterns website, www.darkpatterns.org/
13. Section 5(a) of the FTA Act, www.ftc.gov/about-ftc/what-we-do/enforcement-authority
14. CNIL, Shaping Choices in the Digital World. From dark patterns to data protection: the influence of ux/ui design on user empowerment, April 2019 www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

# 3. METHODOLOGY

The research was conducted in September and October 2019. Three individuals in the EU and two in the US, who will be referred to as mystery shoppers, created new accounts with each of the three selected companies. They followed guidelines developed for this research and captured a range of information and evidence from visiting the selected company websites, opening an account and/or subscribing to services, checking the settings defaults, using the services, and downloading and installing the Android app for each service. In the case of Amazon, the research looked only at the principal shopping aspect and not Amazon music or Amazon Prime for example.

Android apps were chosen because Android is significantly more popular than Apple iOS in the US and EU.[15] Also, research by respected academics and organisations continues to highlight the significant and hidden third-party tracking taking place and leaks of data in Android apps.[16] A decision was taken not to check the iOS apps of each company due to the technical challenges of doing so, in part due to the high security of iOS apps.

Additionally, four individuals in the EU (Belgium and the UK) and six individuals in the US (California and the District of Columbia), which for purposes of this research will be referred to as access volunteers, made requests for copies of their personal data from the companies and recorded their experiences. This was done to help understand how the companies are meeting their obligations to comply with the 'right of access' of their EU based customers under the GDPR (as well as US customers of Spotify, an EU based company) and whether Amazon US and Netflix US extended the GDPR right of access to their US customers.

Finally, we wanted to assess how the companies' current practices regarding their US customers' ability to access their data compares with the data access obligations they will have under the CCPA.

The principal author of this report also conducted both these investigations: mystery shopping and personal information access requests. References to Amazon EU, Netflix EU and Spotify EU in this report apply to research conducted by individuals in the UK and Belgium.

The research used a range of open-source tools to understand whether first-party and third-party tracking for advertising purposes took place on the companies' websites and in their Android apps. These include WebbKoll,[17] a tool that checks the extent to which a website monitors an individual's behaviour and any tracking related to third parties; the Request Map Generator,[18] a tool that helps identify what third parties are present on a site; and Exodus Privacy[19] a tool that analyses Android applications to discover any embedded software use to track the behaviour of individuals and the performance of the app (known as a tracker).

To assess the readability of privacy-related policies and notices, the research used an automated tool[20] and the Flesch-Kincaid Reading Ease and the Flesch-Kincaid Grade Level formulas[21] to gauge how easy or difficult they are to read. In addition to the mystery shopping, subject access requests and analysis of

15. In the US, Android has a 51 per cent market share compared to Apple iOS that has a 20 per cent share. In Europe Android has a 72 per cent market share compared to Apple iOS that has a 29 per cent share.

16. Binns et al, Third-Party Tracking in the Mobile Ecosystem, 2018, www.arxiv.org/pdf/1804.03603.pdf. See also Privacy International website, www.privacyinternational.org/examples/apps

17. Webbkoll website, www.webbkoll.dataskydd.net/en

18. Request Map Generator website, www.requestmap.webperf.tools/

19. Exodus website, www.reports.exodus-privacy.eu.org/en/

20. Readable website, www.readable.com/

21. The Flesch-Kincaid Reading Ease Score has been used by respected computer scientists and academics such as Prof. Lorrie Faith Cranor and colleagues who in a 2009 paper *'Comparative Study of Online Privacy Policies and Formats', argued that the "Flesch index has proven robust in many contexts and we do not immediately see any reason why privacy policies should be dramatically different from other types of textual analysis."* www.robreeder.com/pubs/PETS2009.pdf

legislation, we also acknowledge the research and findings of other organisations who have undertaken similar research and variously referenced in the report.[22] We asked the three companies for initial observations. At the time of publication, Spotify responded, and we are currently engaging with them. We have not received a response from Amazon or Netflix.

# 3.RESEARCH FINDINGS

This section is divided into the key research topics of transparency and an individual's right to be informed and to understand the use of their personal data, consent, data protection by design and default, third-party data sharing, the right of access to personal data and data retention. The topics reflect the research focus, review of the companies' websites, creation of accounts, and installation of the companies' Android apps.

## 3.1 Transparency: Reading privacy policies should not require a high-level reading ability

### 3.1.1 Regulatory framework

Transparency is a cornerstone of data protection law and crucial to help people not only understand how their information will be used to their benefit, but also the risks and safeguards, including any defaults that might impact on their privacy. Transparency is also key in helping people be aware of their rights and how to exercise them.

EU data protection law has long required organisations to process personal data in a manner that is transparent and fair to individuals, reflecting the individual's right to be informed and know about the use of their personal data, and exercise a degree of control over its use.[23] The GDPR[24] strengthened organisations' obligation to be transparent about their use of personal data and strengthened the individual's right to be informed and to know. The GDPR[25] requires organisations to provide individuals with a detailed list of information at the time when their personal data are obtained. This includes, among other things, information about the purposes of processing, the legal basis relied on by an organisation (such as whether the personal data are necessary for the performance of a contract with an individual or whether the organisation relies on consent), the period for which data will be stored and the existence of an individual's rights.

In the US, the CCPA requires businesses to provide individuals with similar information. The California Attorney General has proposed regulations that set out procedures and give guidance that companies should follow to ensure "*consumers' new rights under the CCPA*" are met, such as an individual's right to be informed and to know "*what personal information is collected, used, shared or sold.*"[26]

22. For example: Privacy International website, www.privacyinternational.org/appdata (for technical investigations into app privacy). NOYB.EU *'Netflix, Spotify & YouTube: Eight Strategic Complaints filed on "Right to Access" https://noyb.eu/access_streaming/; Habib et al,* An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites https://www.usenix.org/conference/soups2019/presentation/habib. Norwegian Consumer Council, *Deceived by Design, 27/06/2018,* www.fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf. BEUC website 27/11/2018, www.beuc.eu/press-media/news-events/gdpr-complaints-against-google%E2%80%99s-deceptive-practices-track-user-location (for the co-ordinated GDPR enforcement action with seven national consumer organisations against Google)

23. The EU first introduced a data protection law in 1995, which EU member states implemented in the late 1990s. This law was replaced by the GDPR in 2016 and came into force in May 2018. See European Commission website, www.ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

24. Articles 13 and 14 of the GDPR

25. Article 13 of the GDPR

26. California Consumer Privacy Act, www.oag.ca.gov/privacy/ccpa and CCPA Fact Sheet www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

The GDPR also requires organisations to provide information in a way that is concise, transparent, intelligible and in an easily accessible form, using clear and plain language and that is easy to understand.[27] Similar to the GDPR, the CCPA requires a business to inform individuals about the collection and use of their personal information and their rights in a form that is reasonably accessible.

### 3.1.2 Accessibility and readability of information

The research reviewed the applicable privacy policies, cookie policies and other relevant notices, such as any advertising notices to assess how the companies are meeting their key transparency obligations under the GDPR and the CCPA, as described in section 3.1.1 above. We sought to understand if these policies are easily accessible, clearly signposted and easy to navigate, read and understand. In their guidance on transparency under the GDPR, EU Data Protection Authorities, recognising the role of readability testing, advise that if organisations "*are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing.*"[28]

The readability of the privacy policies and notices was tested using the Flesch-Kincaid Readability formula.[29] The higher the score, the easier the text should be to read and understand. On a scale of 0 to 100, a score of 30 – 49 is considered difficult to read.[30]

As per Table 1 below, the companies' privacy policies, notices, cookie policies and terms of use scored between 35 – 47, meaning that they are difficult to read.

The main privacy policies/notices of the three companies we studied are approximately 3800 – 4700 words long, and that would take between 17 – 21 minutes each to read. That would generally not be considered concise nor easy to understand.

| Company | **Document Type (sign up)** | **Number of Words** | **Time to Read** | **Flesch-Kincaid Reading Ease** |
|---|---|---|---|---|
| **Amazon UK** | Privacy Notice | 3863 | 17.10 | 40.4 |
| | Cookie Notice | 419 | 1.51 | 47.7 |
| | Interest-Based Ads notice | 527 | 2.20 | 39.4 |
| | Conditions of Use & Sale | 6459 | 27.31 | 44.5 |
| **Amazon US** | Privacy Notice | 2671 | 11.52 | 46.2 |
| | Conditions of Use | 3391 | 15.04 | 39.6 |
| **Netflix UK** | Privacy Statement | 4285 | 19.02 | 35.0 |
| | Terms of Use | 2267 | 10.04 | 45.9 |
| **Netflix US** | Privacy Notice | 3999 | 17.46 | 35.6 |
| | Terms of Use | 4057 | 18.01 | 40.9 |
| **Spotify UK** | Privacy Policy | 4738 | 21.03 | 43.2 |
| | Terms and Conditions of Use | 8457 | 37.35 | 35.6 |
| | Cookie Policy (access to site) | 1860 | 8.16 | 43.6 |
| **Spotify US** | Privacy Policy | 4728 | 21.0 | 43.3 |
| | Terms and Conditions of Use | 7469 | 33.11 | 36.2 |

***Table 1: A Flesch Reading Ease score of 30-49 is considered difficult to read***

27. Article 12 and Recital 39 of the GDPR that additionally require that information and the communication of information should be "easy to understand [using] clear and plain language [and that individuals] should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights" especially in the case of online advertising (Recital 58).
28. Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), DG Justice and Consumers European Commission website, www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
29. Readability Formulas website, www.readabilityformulas.com/flesch-reading-ease-readability-formula.php
30. Pearson Clinical website, www.pearsonclinical.co.uk/Sitedownloads/Miscpdfs/Gradetoage.pdf

In addition to poor readability, the companies' policies and notices that were analysed during the research were not found to make essential information, key choices and rights easily accessible or easy for consumers to use. Not only does this appear to not meet the requirements of the GDPR, but it also does not appear to meet guidelines issued by the EU data protection authorities on transparency under the GDPR.[31] In those guidelines, the data protection authorities emphasise that *"the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to [individuals]."*

Based on our mystery shopper research, and if the results were to be extrapolated, it would suggest that companies do not meet this crucial aspect of the GDPR and CCPA and the draft CCPA regulations, meaning that individuals may not be aware of the consequences of the use of their data or of any safeguards they may be able to take.

### 3.1.3 Communicating information about the use of personal data and rights

Though the privacy 'policies' or 'statements' or 'notices',[32] as variously named by the three companies that were analysed, raise concerns as set out in this report, the privacy notices of Netflix and Spotify at least seem to be the same for customers in the EU and US. These two companies appear to adopt the same practices irrespective of whether a customer lives in the US or the EU.

Amazon however, does not apply the same policies and practices to customers in the EU and the US. There are some important differences between the two entities. Unlike Amazon EU, the privacy notice of Amazon US was found not to set out the purposes for which personal information is processed. Nor did it provide any right to request access to personal information or other rights that apply to customers of Amazon EU. This was the case for the mystery shopper in California as well as in Washington D.C. Also, unlike customers of Amazon EU, customers of Amazon US do not have any mechanism to request a copy of their personal information (see also section 3.5 right to access of personal data below). The right to know the purposes of processing and to obtain a copy of personal information are requirements of the CCPA (see section 3.1.1 above) that will take effect from January 2020.[33]

#### Signposting information

While Amazon and Spotify were found to adopt a layered approach in their privacy notices, setting out key themes under separate headings about what personal information is 'collected', those individual sections tend to use long sentences and structure that is hard to read and understand. Individuals must also still seek out further specific details of purposes, legal basis and how to exercise their rights, including the right to access their personal information. This does not help people make informed decisions about the use of their personal data or exercise their rights easily.

As explained above (see 3.1.1.), the GDPR requires organisations to clearly set out in an accessible way, using plain language the *specific purposes and specific legal basis* for the processing of personal data.[34] Unfortunately, while the privacy notices of Amazon EU and Spotify EU/US set out the purposes of processing under distinct headings they describe the purposes in a generic way. The research found that Amazon EU for example, does not explain the specific purpose for which personal data is used and on what legal basis under the GDPR. This may prevent individuals from making informed decisions about the use of their personal data and understanding the implications of such use.

The Netflix EU and US privacy notice is more problematic. Information was not found to be signposted in any way. This means that by default, individuals must search for information about specific matters such as the purposes of processing, user rights, and access to data. The Netflix privacy notice also advises that personal information may be processed for "*other purposes described in the Use of Information section of this Privacy Statement*", but such purposes are not expressly defined in the statement.

---

31. See footnote 28.
32. The three companies use the terms Privacy Notice, Privacy Policy and Privacy Statement to describe how they use personal data and any applicable rights. This report will refer to these commonly as a Privacy Notice.
33. California Consumer Privacy Act, www.oag.ca.gov/privacy/ccpa
34. Article 5(1)(b) requires that "personal data shall be collected for specified, explicit and legitimate purposes"

The Spotify EU and US privacy policy is an improvement on those of Amazon and Netflix. Spotify EU and US sets out in a table format: 1. the purpose of processing; 2. the legal basis of processing; and 3. the categories of personal data. However, it remains unclear precisely what personal data is processed, for what specific purpose, and on what specific legal basis. The individual sections are also difficult to read and do not clearly signpost or facilitate the easy exercise of individual rights.

**Purposes and legal basis for data collection**

Spotify, in Section 6 of its privacy policy, entitled 'what do we use your personal data for?', says it uses account registration data and service usage data for a broad range of purposes. These purposes include providing personalised or localised content and advertising on or outside of Spotify including for third-party products. Service usage data includes information about an individual's interactions with the Spotify Service such as "*the date and time of any requests you make, songs you have listened to, playlists you create, video content you've watched [and] URL information, cookie data, your IP address, the types of devices you are using to access or connect to the Spotify Service, unique device IDs, device attributes*."

Spotify says the processing of this data is necessary for the performance of a contract and its legitimate interests. However, in its privacy policy, Spotify does not notify individuals of the right to object to the processing of personal data or provide a means for individuals to object, and questions whether the company is meeting its obligations under the GDPR. As described in section 3.1.2, Spotify's privacy notice is scored as generally difficult to read. The specific text about the use of account registration data and service usage data to personalise the service, including for advertising on or outside of Spotify, has a Flesch-Kincaid Reading Ease score that makes it very confusing to read.

This research found that Amazon EU does not set out the legal basis relied on for the processing of personal data. The mystery shoppers also found Netflix EU/US ambiguous and lacking specificity to enable the mystery shoppers to understand in an easy manner what data will be used, for what specific purposes, and on what legal basis. This would appear to be in contradiction of guidelines[35] issued by the European Data Protection Board (EDPB)[36] on the processing of personal data for the performance of a contract for example. EU Data Protection Authorities advise that the purposes of processing must be "*clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose*" and that "*in line with their transparency obligations, controllers should make sure to avoid any confusion as to what the applicable legal basis is*." This is also applicable not just to Amazon EU but also to Netflix EU and Spotify EU/US. None of the companies appear to clearly set out what personal data is used for and the legal basis of its use in a way that satisfies the requirements of the GDPR or the EDPB guidelines.

**Tracking and profiling information**

The EDPB[37] also advises that "*as a general rule, [the] processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services.*" This is important because each of the companies tracks individuals for behavioural advertising from the moment an individual first visits their websites and throughout their use of the companies' services, as defined by this research. It is unclear what legal basis the companies rely on for these purposes under GDPR, for example, for the performance of a contract or the companies' legitimate interests.

The research also found that each of the companies use a range of behavioural data such as an individual's listening, viewing, search, and browsing activities to support personalised and behavioural advertising, including third-party advertising. The data may also include interest-based and online advertising-related data obtained from third parties. The companies also set a range of defaults that

35. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 08/10/2019, European Data Protection Board, October 2019, www.edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

36. About the EDPB, European Data Protection Website, www.edpb.europa.eu/about-edpb/about-edpb_en

37. See footnote 31, The guidelines also state that *"where personalisation of content is not objectively necessary for the purpose of the underlying contract, for example where personalised content delivery is intended to increase user engagement with a service but is not an integral part of using the service, data controllers should consider an alternative lawful basis where applicable."*

serve the purpose of targeted advertising and direct marketing. These defaults are set without making individuals aware in a clear and transparent manner of their existence, their implications, and of the rights and choices individuals have in that regard.

The privacy notices of all three companies were found to be silent on the data involved and consequences of profiling and/or automated decision-making.[38] The companies also do not notify individuals of the right to object to profiling for direct marketing purposes, which would include profiling for behavioural advertising purposes.[39] As all three companies engage in the personalisation of services and behavioural targeted advertising, it is difficult to understand how these activities can take place without the help of profiling and/or automated decision-making.

The GDPR requires companies not only to tell individuals in a clear and transparent manner about these activities, but also, according to EU data protection authorities, the obligation to explicitly bring the right to object to profiling for direct marketing purposes to their attention.[40] The right to object must be presented clearly and separately from any other information. None of the companies was found to currently be meeting this important obligation.

If companies do not provide information in a clear manner, or through simple, clear processes, individuals will be unable to easily exercise their rights and control over their personal data. Thereby impacting on an individual's privacy and rights.

The assessment carried out for this report suggests that from an EU GDPR perspective the privacy policies of each company do not meet the core transparency obligation to notify individuals of the specific purpose and specific legal basis relied on.[41] Not specifying the purpose of processing and the data involved, especially about third-party advertising, also raises questions about the degree to which the companies will be in a position to meet their obligations under the CCPA.

**To conclude**, none of the selected companies make it easy to understand what data is used for what specific purposes. Their privacy policies and associated policies on cookies or interest-based ads are hard to read. They are ambiguous in key places and do not specify precisely what personal data is used and for what purpose, making them difficult to understand. The rights and choices of individuals were not found to be communicated in a manner that makes them easy to exercise. Some uses of personal data and marketing and advertising defaults are hidden from view.

Laws such as the GDPR (and soon the CCPA) oblige companies to review their privacy policies and provide individuals with more information. Some companies attempt to layer their policies to make it easier for individuals to find the most important information. This does not necessarily lead to better readability, understanding or choice, however.

**Recommendations – transparency and the right to be informed**

- Companies should test the readability of their policies. They should also conduct user interface and user experience testing to ensure the interests and needs of individuals are met in an easy manner.
- Companies should design transparency in by default beyond the privacy policy, for example, by expressly bringing to the attention of individuals any defaults used to automatically track, profile and target individuals for advertising.
- Regulators should consider how to support a standardised approach and issue guidelines that link transparency to the obligation to ensure data protection by design and default.

38. Profiling means the automated processing of personal data in order to analyse and/or predict certain things about an individual such as their interests, personal preferences, behaviour, location or movements.

39. Article 21(3) and Recital 70 of the GDPR

40. European Commission website, www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, p.39-40. See also UK ICO website

41. Article 5(1)(a) and (b) and Article6, Recital 39, Recital 50 of the GDPR

## 3.2 Consent: Pre-ticked boxes do not amount to consent

### 3.2.1 Regulatory framework

The GDPR requires organisations to have at least one lawful basis on which to process personal data. For example, processing personal data that is *necessary* for the performance of a contract with an individual.

Consent is another basis to ensure processing is lawful, but may not always be appropriate or required.[42] The research looked at whether the three selected companies relied on consent as a lawful basis and if so, whether such consent met the standards set out in the GDPR and applicable regulatory guidance.[43]

Transparency is also an 'essential condition' for ensuring consent is valid in law and as argued by EU data protection authorities.[44] This means that a request for consent:

- Must be presented in a manner that is intelligible, easily accessible, and uses clear, plain language.[45]
- Must be as easy to withdraw consent as it is to give it
- An individual must give consent pro-actively. Pre-ticked boxes or slider buttons set to ON do not amount to consent.

In addition to the GDPR, the research considered the application of the ePD that regulates the use of cookies and similar technologies such as tracking pixels that companies may put on their websites.[46] The research also considered recent cookie guidance issued by the UK,[47] French[48] and Dutch[49] data protection authorities, and a recent ruling of the Court of Justice of the EU called the Planet49 case.[50]

The ePD, EU case law (such as Planet 49) and regulatory guidance require opt-in consent for organisations to store information on or access information stored on people's devices, such as setting cookies for behavioural advertising purposes. Consent is not required if the storage or access is *strictly necessary* to provide a service expressly requested by an individual. Consent required under the ePD, must meet the standard on consent set out under the GDPR.[51]

The CCPA, unlike the ePD, does not require consent for the use of advertising cookies and instead relies on users opting out of their data being shared with third parties. However, the CCPA does require companies to provide users with a notice about such sharing and the option to opt out of it.

### 3.2.2 Analysis of privacy policies

In their privacy policies all the companies were found to advise that they may use an individual's personal data with their consent. However, apart from Spotify's explanation of 'voluntary mobile data', the policies are ambiguous and do not set out precisely what personal data and for what purposes they rely on consent for. Understanding what the companies rely on consent for or how to withdraw consent was unclear.

---

42. Article 6 of the GDPR

43. Article 7 of the GDPR and Article 29 Working Party Guidelines on consent under Regulation 2016/679 www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (cross reference to footnote 28) endorsed by the European Data Protection Board www.edpb.europa.eu/our-work-tools/our-documents/guideline/consent_en

44. Article 29, Working Party Opinion 15/2011 on the definition of consent, 13/17/2011, www.ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

45. Article 7 of the GDPR

46. Directive 2002/58 EC as amended in 2009. Consolidated version www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A02002L0058-20091219

47. UK Information Commissioner, Guidance on cookies and similar technologies, July 2019 www.ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/

48. CNIL, Cookies and other tracking devices: the CNIL publishes new guidelines, 23/07/2019, www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines

49. Autoriteit persoons gegeven website, www.autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weiger-en-tracking-cookies

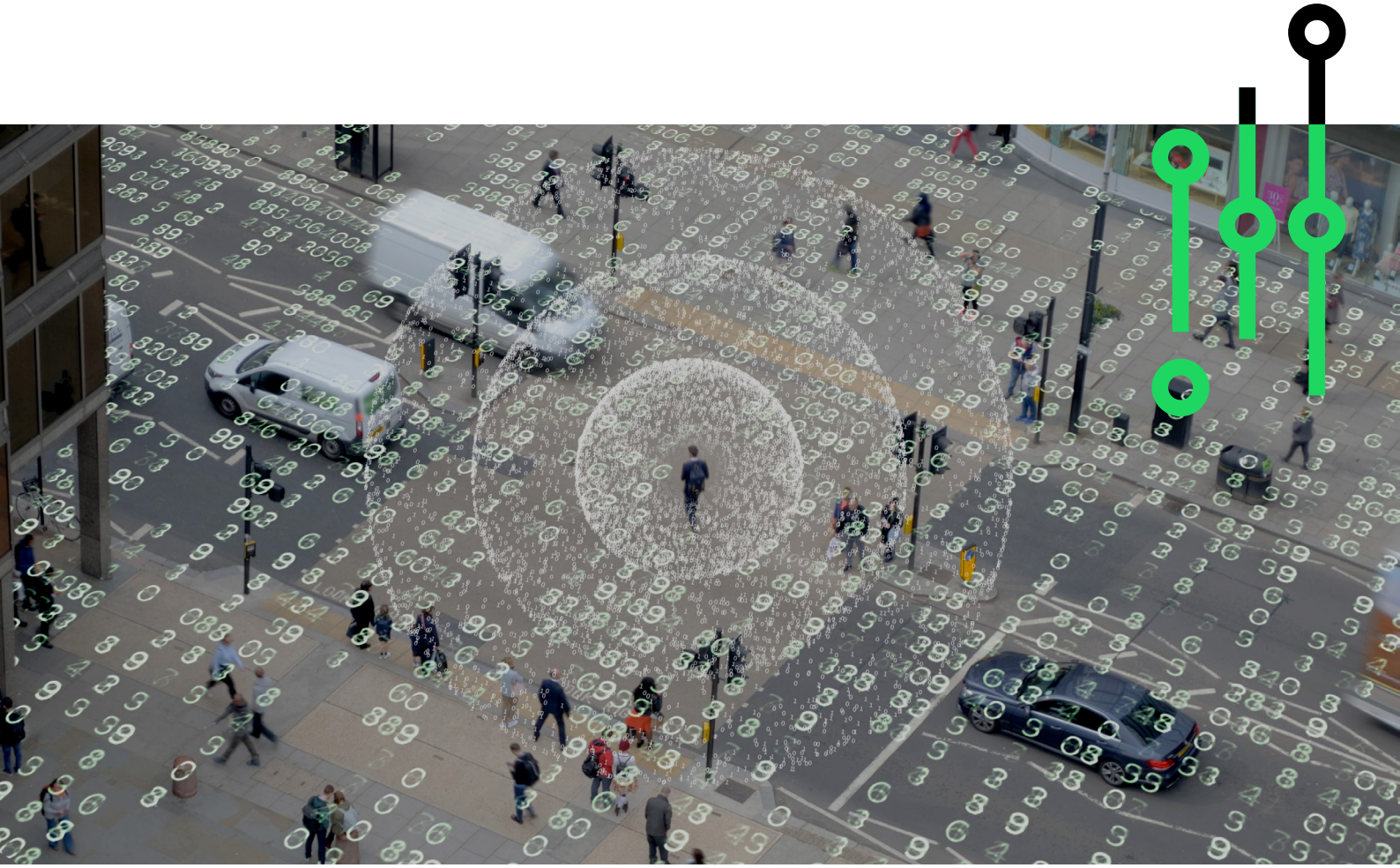
50. Court of Justice of the EU. Case C-673/17 www.curia.europa.eu/juris/liste.jsf?num=C-673/17

51. EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, www.edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

**Amazon EU/US**

Amazon EU advises it "*may also ask for your consent to process your personal information for a specific purpose that we communicate to you*," but does not set out anywhere what purposes it relies on consent for.[52] Nor was the company found to refer to consent in its cookie notice,[53] though the company does set cookies for advertising purposes that require consent under EU law. Instead, it presents a less-than-obvious cookie notice that advises "*We use cookies to provide and improve our services. By using our site, you consent to cookies*." Cookies are used for a range of purposes including "*ads, relevant to your interests on Amazon sites and third-party sites.*"[54] This practice does not meet the ePD, case law and regulatory guidance in the EU.

Amazon US was found to advise its customers that they will be notified when information about them goes to third parties and can at that point choose not to share. It calls this "*with your consent.*"[55] Amazon US also does not refer to consent in the cookies section of its privacy notice, or its interest-based ads notice,[56] though the company sets cookies for *"personalised advertisements on other Web sites."*



52. Amazon Privacy Notice, www.amazon.co.uk/gp/help/customer/display.html/ref=ap_desktop_footer_privacy_notice?ie=UTF8&nodeId=502584
53. Amazon cookies, www.amazon.co.uk/gp/help/customer/display.html/?nodeId=201890250
54. Amazon Interest-based Ads, www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=201909150&ref_=footer_Interest_Based_Ads_Notice
55. Amazon Privacy Notice, www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy
56. See footnote 54

### Netflix EU/US

Based on our research, we found that Netflix has the same privacy statements for both US and the EU, which is to be commended. It generally mentions that it will request consent for certain 'consumer insights' activities, and that such consent can be withdrawn at any time. Activities listed include processing personal data for 'surveys'.[57] However, Netflix does not ask for such consent when it automatically sets a range of 'communication settings' defaults to ON via the use of pre-ticked boxes. Individuals are required to opt-out of these boxes, including 'Netflix Surveys'. At no point during a new sign-up process does Netflix advise of these settings. Based on our research, we do not believe that the companies are meeting the requirement for transparency and conditions for consent, pre-ticked boxes do not amount to consent under EU law (section 3.2.1) for example. See Image 1 below.

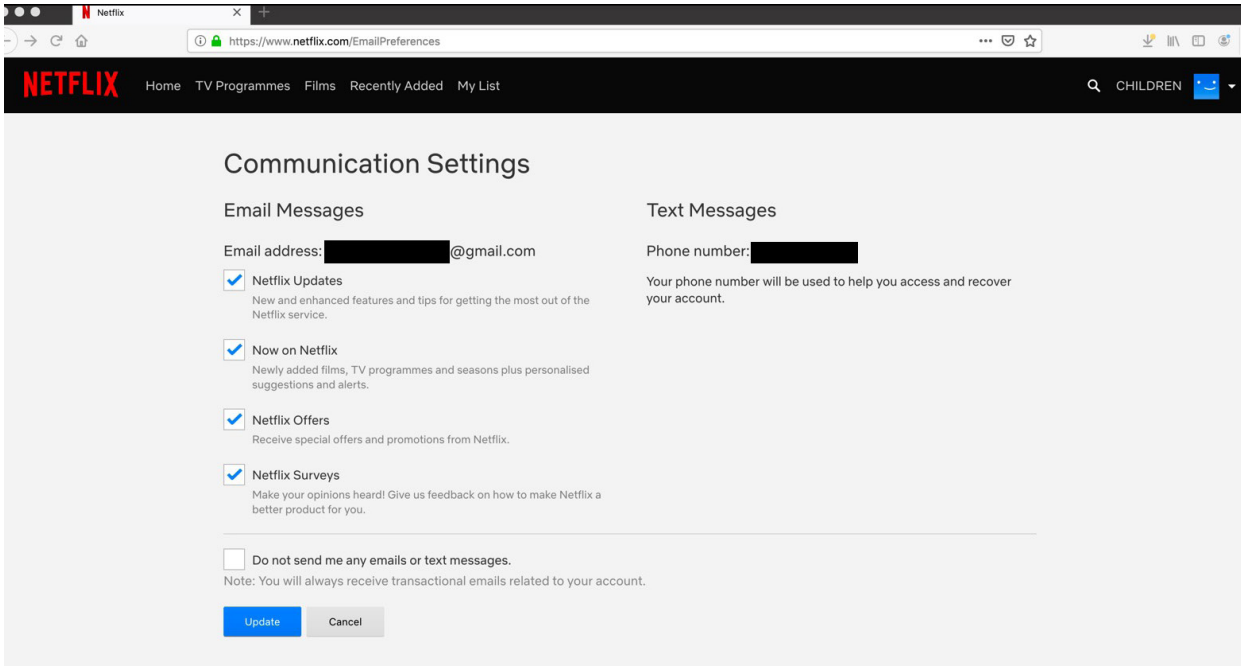



***Image 1: Netflix UK Communications Settings. Defaults ON***

Further, in sections referring to user information and rights, the information Netflix provided was found to be ambiguous to the point of being rated as 'very confusing' under the Flesch-Kincaid Reading Ease formula (a score of 29.5, see section 3.1.2 above). It is not clear from the company's privacy statement[58] the purpose for which it relies on consent as a lawful basis under the GDPR. This may affect negatively an individual's ability to read and understand the uses of their data and available choices that may impact their privacy and rights.

57. Netflix Privacy Statement, www.help.netflix.com/legal/privacy
58. Ibid

### Spotify EU/US

As an EU-based company, Spotify must conform to GDPR for its customers in the EU and the US, consequently its privacy policy is the same for both. However, its privacy policy was found to be ambiguous and from a readability perspective, scored as 'very confusing' in the section on rights and preferences.[59] Except for a section on the use of 'voluntary mobile data' it is unclear the circumstances under which Spotify would ask for (opt-in) consent.

Spotify sets to ON the defaults for a number of 'Notification settings' using pre-ticked boxes for email and push communications that are predominantly related to direct marketing. See Image 2 below. At no point were the mystery shoppers made aware of the setting of these default choices, nor were they prompted to give their consent or even to opt-out. This process does not meet the requirements of the ePD or the transparency requirements of the GDPR.

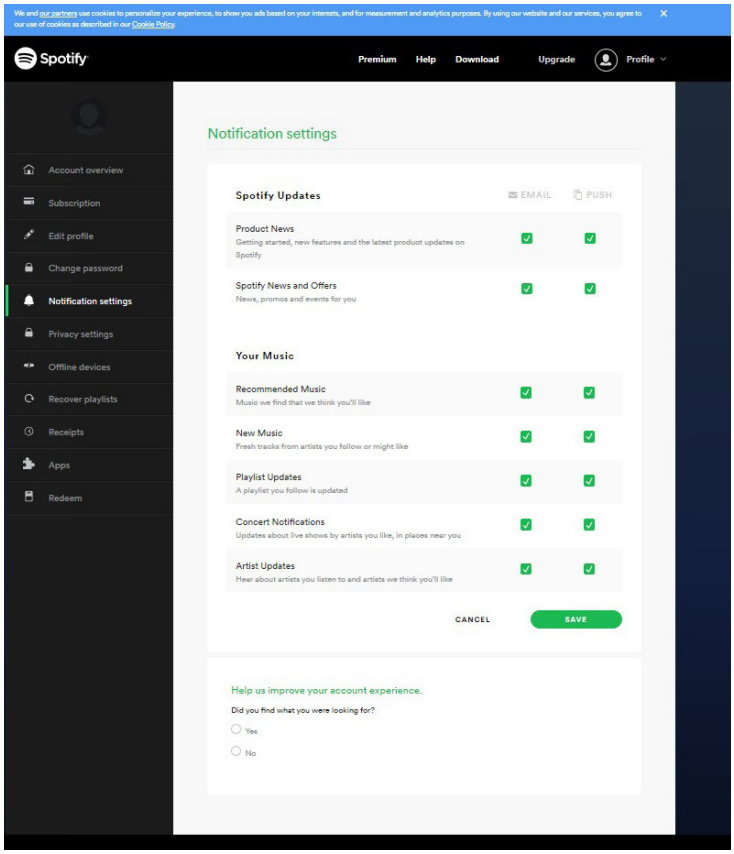



***Image 2: Spotify Notification Settings. Defaults ON***

### 3.2.3 Mystery shopping

In addition to reviewing the privacy policies and cookie and advertising notices for each company, the mystery shoppers also opened new accounts with each company in the EU and the US. This was to test how the companies inform customers of key uses of their personal data, whether they use defaults that may impact on privacy, whether they rely on consent, and how easy it is for individuals to exercise rights.

### Tracking website activity for behavioural advertising

When the mystery shoppers visited the Amazon, Netflix and Spotify websites, their online activity was automatically tracked by the companies and by a range of third parties for advertising purposes based on their behaviour.

Only mystery shoppers visiting the companies' EU-based sites were given a cookie notice advising that cookies are used for such advertising. None of the companies appear to obtain consent for behavioural-based advertising as they should be doing under EU law. Even just visiting the companies' privacy policies on those sites is taken as consent to tracking for advertising.The Webbkoll transparency tool revealed that the home page of Amazon EU's site,[60] involved 7 first-party, 42 third-party cookies and 303 third-party requests to 38 different third-party domains other than Amazon EU.

59. Spotify Privacy Policy, www.spotify.com/uk/legal/privacy-policy/ Section "Your rights and your preferences" scored difficult to read under the Flesch-Kincaid Reading Ease formula

60. Amazon website, www.amazon.co.uk/ visited on 22/09/2019 at 12.31:03 ETC/UTC

During the mystery shopping exercise, the companies' US sites did not appear to present any notice about the use of cookies or other techniques for targeted advertising. Tracking took place without telling people or giving them clear choice. For example, the Webbkoll transparency tool revealed, on the Amazon US site,[61] 9 first-party, 48 third-party cookies and 316 third-party requests to 42 different third-party domains other than Amazon. Similar tracking was discovered also on the US sites of Netflix and Spotify and on the EU sites of all the companies.

See Table 2 below. Companies were found to be less immediately open and transparent with their US customers than their EU customers about online tracking for advertising. For example, US customers did not get any cookie notices when they first visited a site.

| | **Amazon UK** | **Amazon US** | **Netflix UK** | **Netflix US** | **Spotify UK** | **Spotify US** |
|---|---|---|---|---|---|---|
| Is advertising-related tracking present on the home page? | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Prominent 'cookie' notice? | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ |
| Is opt-in consent requested for ad-related tracking? | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Is third-party ad-related tracking present? | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Is the Facebook Pixel present? [62] | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Tracking detected on the home pages by the Webbkoll transparency tool (30 October 2019) | 7 first -party & 40 third -party cookies. 352 third -party requests to 37 unique hosts | 9 first -party & 44 third -party cookies. 339 third -party requests to 42 unique hosts | 7 first -party & 3 third-party cookies. 30 third -party requests to 11 unique hosts | 7 first -party & 4 third -party cookies. 31 third -party requests to 12 unique hosts | 20 first-party & 20 third -party cookies. 118 third -party requests to 50 unique hosts | 20 firs -party & 20 third -party cookies. 122 third -party requests to 50 unique hosts |

61. Amazon website, www.amazon.com visited on 17/09/2019 at 17.21.51 ETC/UTC
62. A Facebook Pixel is software code placed on a website that is used to track the actions people take on a website in order to target them on Facebook and to measure the effectiveness of that advertising www.facebook.com/business/help/742478679120153?id=1205376682832142

### Tracking use of services for behavioural advertising

The research also found that when the mystery shoppers created accounts, Spotify EU/US and Amazon EU/US automatically set to ON some defaults that the companies use for their own and for third-party behavioural advertising purposes. The mystery shoppers were not told about these defaults, that were not in any way obvious and appeared hidden from plain view. See image 3 for Amazon US default.

It is not clear if turning off these defaults stops the profiling and use of data for advertising purposes or if it only stops the targeting of ads based on data about how people use the services. This reflects the ambiguity of related privacy policies and text used to support marketing and advertising-related default settings.

When the mystery shoppers installed the Spotify desktop app, the company was found to:

- Set a Spotify Advertising cookie that "*Enables Spotify ads tailored to your interests and preferences.*" This can be revoked, but in the experience of our mystery shoppers, was difficult to find in the account and app section of their profile. See image 4.
- Set to ON a hidden default in the company's desktop app. This default allows the company to set cookies to track how individuals use the app for purposes that includes interest-based and targeted advertising. This default is hidden in the advanced settings page of the app. Through the process our mystery shoppers were not advised that an advertising cookie will be set by Spotify when installing the app on their computers. See image 5.

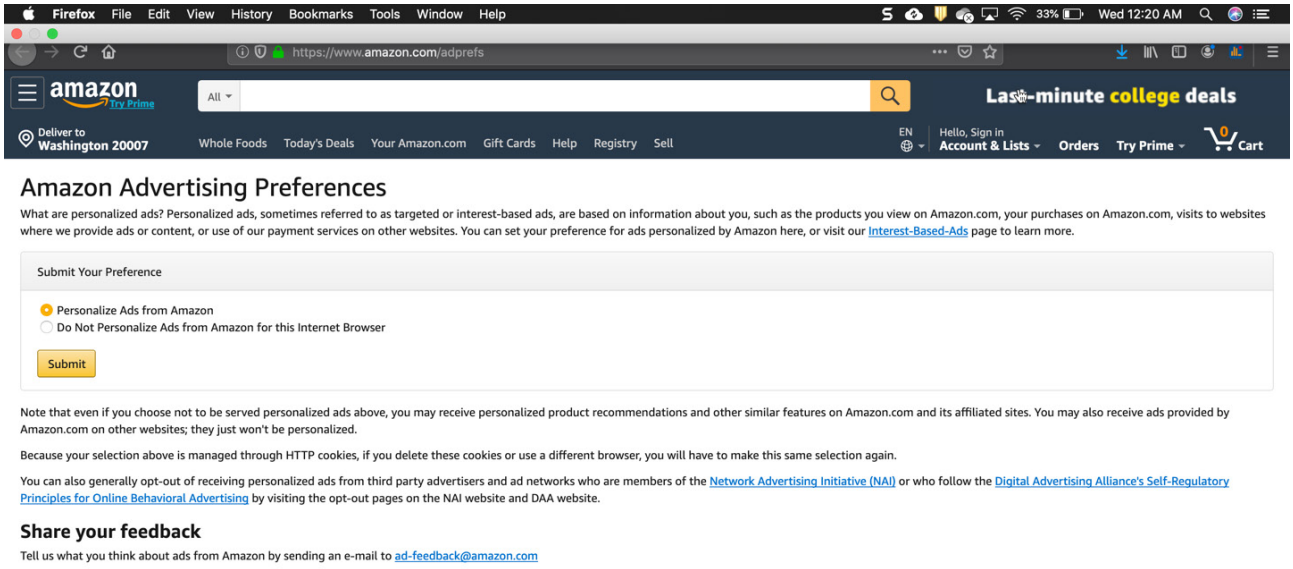



***Image 3: Amazon US Advertising Preferences***

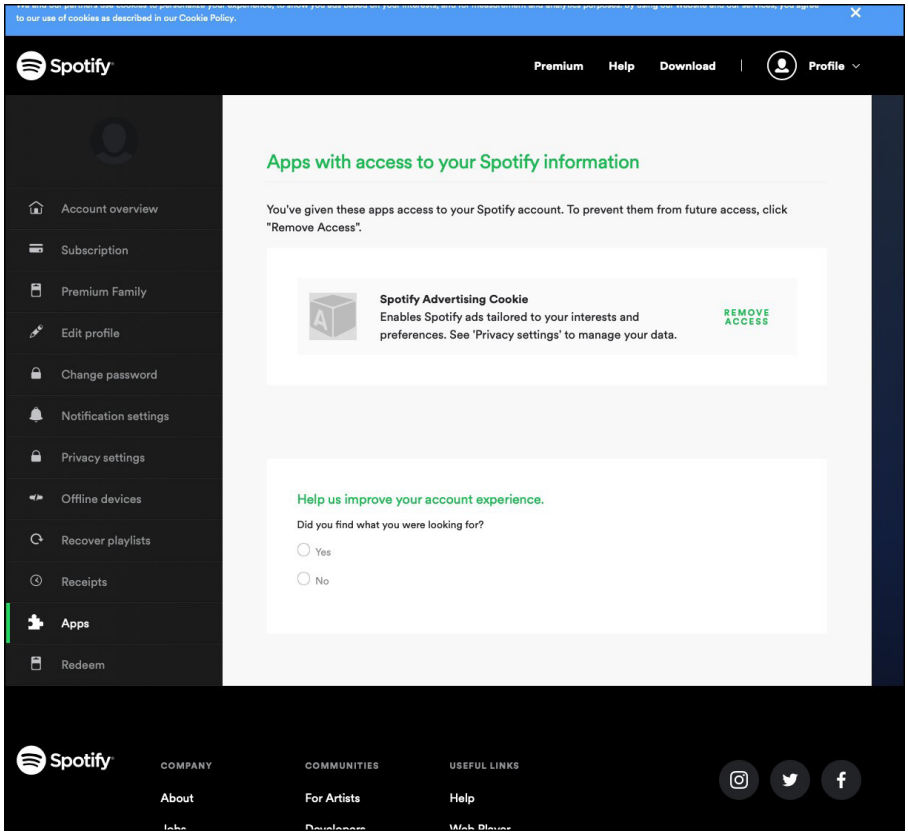



***Image 4: Spotify Advertising Cookie – desktop app***

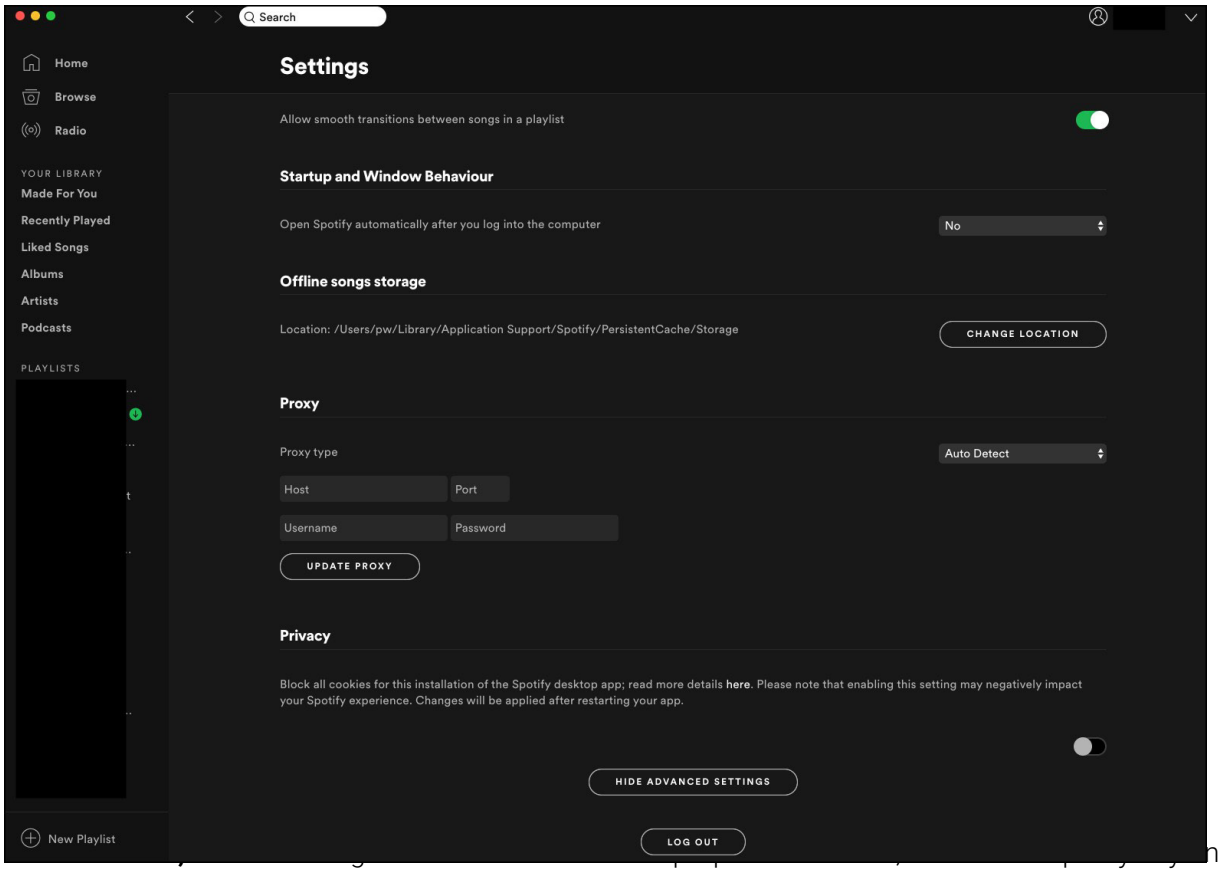



***Image 5: Spotify desktop app cookie tracking default***

consent. They were found to be ambiguous, for example, about whether they rely on consent or another basis for the third-party advertising activities and/or the tracking defaults highlighted above. In the experience of our mystery shoppers, it was difficult for individuals to understand if and what they are consenting to.

The three companies also appear to use cookies and other techniques and default settings for multiple purposes, bundling these together without specific choices being available to individuals. They use different terms for similar purposes but do not describe them clearly nor are they clear about what data is used in relation to these terms or purposes. For example, 'personalised experiences', 'interest-based advertising', 'targeted advertising', 'tailored advertising', and 'marketing' are all used interchangeably.

**Recommendations:**

- Companies should clarify when the use of people's data is based on consent and meet the standards of consent set out in the GDPR and as referenced in this report.
- Companies should review their use of cookies and other tracking techniques, and their use of pre-set defaults in light of the ruling of the Court of Justice of the EU in the Planet 49 case,[63] in which the Court ruled that pre-ticked boxes do not amount to consent and that the use of data for different purposes cannot be bundled under the same consent.
- Companies should provide clear and conspicuous notice about the use of tracking defaults described in this report and not engage in tracking for behavioural advertising unless an individual gives their consent.
- Companies should review their privacy, cookie and advertising notices and be clear and consistent in their use of terms such as personalisation and interest-based advertising, and make the information about the data involved and the choices and rights easily available and clear.
- In the EU, the EDPB should develop guidance on the use of cookies and consent.
- EU national data protection authorities should enforce rules on online tracking and the use of defaults.
- In the US, the CCPA implementing regulations should provide clear rules on the notice requirements for the use of cookies for third-party advertising.

63. Curia website, www.curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&-mode=req&dir=&occ=first&part=1&cid=1447493

### 3.3 Data protection: Privacy should not be an advanced setting

The GDPR expressly obliges organisations to consider and build data protection into business practices, systems and processing operations and ensure that by default only personal data necessary for a specific purpose (specified in the privacy notice, for example) is actually processed.[64] The use of privacy invasive default settings can have significant implications for an individual's privacy and may result in the processing of their personal data in ways they do not expect, or that may negatively impact on their privacy.

This report looked at whether privacy-related settings were set to ON or OFF by default, what data they related to, and how transparent, obvious and accessible this information was. The research considered the degree to which the companies' practices may be considered so-called 'dark patterns' through for example, the use of "*interfaces that can confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions.*"[65]

As discussed above (see 3.2.3, Mystery shopping), these three companies were found to track the mystery shoppers from the point of first visiting their websites. Tracking continued through the setting of advertising and marketing defaults that were not obvious to the mystery shoppers and that may be hidden from view; for example, in 'advanced settings'. Privacy should not be an 'advanced setting' – it should be the default setting.

Certain design choices and defaults observed do not appear centred on the individual. Amazon and Spotify use language that may have the effect of dissuading their users from disabling privacy-invasive defaults or cookies by suggesting negative effects or limitations of use. For example, in its cookie notice, Amazon EU advises that "If *you disable all cookies on your browser, neither we nor third parties will transfer cookies to your browser. If you do this, however, you may have to manually adjust some preferences every time you visit a site and* ***some features and services may not work***" (authors' emphasis). Spotify EU/US advises those who seek to disable cookie tracking in the desktop app, "*that enabling this setting* ***may negatively impact your Spotify experience***," (authors' emphasis) but without explaining in what way.

**To conclude**, the default settings do not appear to put consumer interests and rights first and foremost, which is contrary to their obligations under the GDPR. All three companies investigated apply default settings that allow the use of peoples' data for interest-based advertising, which may include sharing the data with third-party advertising partners. These defaults were not made obvious to the mystery shoppers and were hidden from plain view. The existence of such default settings and the resulting consequences may or may not be referenced in privacy policies or cookie notices and are too ambiguous for individuals to understand in meaningful ways. It is also unclear if turning off advertising-related defaults stops the underlying profiling or data sharing. For example, with third parties (see section 3.4 below).

**Recommendations - data protection practices:**

- Companies should review the default settings on both their EU and US sites and apps that support the automatic profiling and targeting of individuals for advertising purposes.
- Companies should ensure transparency through prominent ad tracking information and direct signposting to decision-making buttons or tick boxes.
- Companies should test the clarity and accessibility of this information with individuals.

64. Article 25 Data Protection by Design and Default. Recital 78 of the GDPR

65. George J. Stigler Center for the Study of the Economy and the State. The University of Chicago Booth School of Business, Report of the Committee for the Study of Digital Platforms Privacy and Data Protection Subcommittee, July 2019, www.research.chicagobooth.edu/-/media/research/stigler/pdfs/data---report.pdf?la=en&hash=54ABA86A7A50C926458B5D44FBAAB83D673DB412

## 3.4 Third-party tracking: The more we stream, the more they learn

The sharing of personal data with third parties for the third parties' own uses of the data is not always obvious and may be a concern to individuals, as may 'partnerships' that facilitate third-party tracking and targeting of people for advertising. The research reviewed the policies of the companies for their approaches to lawful basis,[66] transparency, and choice and control with regards to sharing data with third parties. For example, how obvious is such sharing? How is it signposted? What options are available and how easy is it for participants to understand and change the pre-set options? What are the defaults for data sharing?

> In guidance on transparency under the GDPR, the EU data protection authorities advise that "*In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data.*"[67]

Currently it is impossible to answer these questions from the information that these three companies provide. For example, Amazon US advises individuals that "*If you do not want us to use personal information that we gather to allow third parties to personalise advertisements we display to you, please adjust your Advertising Preferences.*"[68] However, Amazon does not identify what personal information is used or what third parties are involved.

Netflix says it discloses information for *"certain purposes and to third parties,"* but it is not clear what third parties, what personal data is involved or what lawful basis the company relies on.[69]

Spotify says it may share information with "*service providers and others*" but does not clearly set out who the 'others' are. For example, it is unclear if 'others' includes partnerships such as the WPP Data Alliance, with which Spotify reached an agreement in 2016 to harness "*insights from the connection between music and audiences' moods and activities," based on the "unique listening preferences and behaviours of Spotify's 100 million users in 60 countries.*"[70]

The lack of clear and specific information about who Spotify shares data with and for what purposes undermines the ability of individuals to understand how their data are used and to exercise their rights over their data. For example, Spotify has distinct brand[71] and custom audience interest-based advertising businesses.[72] These Spotify ad businesses allow the targeting of individuals based on age, gender, language, location and platform, streaming behaviour "*alongside their broader interests and behaviors, fueled by leading third-party data providers in select markets.*"[73] Spotify for Brands says *"The more they stream, the more we learn. User engagement fuels our streaming intelligence — insights that reflect the real people behind the devices. These real-time, personal insights go beyond demographics and device IDs alone to reveal our audience's moods, mindsets, tastes and behaviors."*

To conclude, the research found that the privacy policies of all three companies, both in the EU and the US, do not provide sufficient and specific information on any third parties with which data is disclosed to or shared with, in order to ensure the use of personal data is transparent and fair to individuals.

---

66. For example, the EU Article 29 Working Party, in its Opinion 4/2012 on Cookie Consent Exemption, asserted that "Third-party cookies used for behavioural advertising are not exempted from consent as already highlighted in detail by the Working Party in Opinion 2/2010 and Opinion 16/2011" www.ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
67. EU data protection authorities Guidelines on transparency under Regulation 2016/679 www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
68. Amazon website, www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy
69. Netflix website, www.help.netflix.com/legal/privacy
70. WPP's Data Alliance and Spotify announce global data partnership, PR Newswire,15/11/2016, www.prnewswire.com/news-releases/wpps-data-alliance-and-spotify-announce-global-data-partnership-300362733.html
71. Spotify for Brands website, www.spotifyforbrands.com/en-US/audiences/
72. Spotify Ad Studio website, www.adstudio.spotify.com/audience-targeting#what-is-targeting-by-interests
73. See footnote 71

## 3.5 The right of access to personal data

The right to obtain a copy of personal data processed by organisations is provided in data protection laws around the world. Both the GDPR[74] and the CCPA[75] give individuals the right to access their personal data, to know about its use, and to obtain a copy of the data in a format that is easy to understand.[76] There are some significant differences between the two however. For example, the CCPA only requires specific information for the previous 12 months to be provided on request, while the GDPR has no such time limits.

A point our research found not to be reflected in the practices of Amazon EU, Netflix EU/US and Spotify EU/US is that the GDPR applies to personal data undergoing processing,[77] not just to personal data the companies hold. The companies' procedures for dealing with customers' data access requests appear to be geared to providing data that is held and easily accessible and retrievable.

The research for this report considered the degree to which the companies are meeting their obligations with regards to the 'right to access' including, whether the right is clearly signposted on their sites and therefore easy to find and exercise, what proof of identity is required, and whether all the data that users are entitled to is provided.

To help with the research, and in addition to the analysis of company sites and policies, volunteers in the EU and the US requested their personal data from the companies with which they had accounts and recorded their personal experiences.

74. Article 15 of the GDPR
75. 1798:100(a) of the CCPA
76. Future of Privacy Forum, Comparing privacy laws: GDPR v. CCPA, 2018, www.fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf
77. European Commission website, www.ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en provides an explanation of what constitutes data processing

### 3.5.1 Amazon EU: Prompt response for those who read the small print

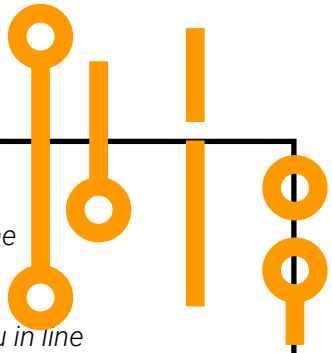
The research found that the US site of the company does not provide for this right, therefore is not included in the below analysis. See the box below for volunteer experiences with Amazon EU.

Amazon EU was only found to refer to the right to request access to personal data as a footnote to a section in its privacy notice called 'What choices do I have'. The notice does not contain any reference to the right to obtain a copy of personal data. Our access volunteers were given examples of information collected by Amazon, but in their experience, there was no reference to other data such as inferred data, profiling data, or data obtained via its extensive advertising network and activities.

We found that it is not easy to exercise the right of access: individuals either have to read through a long privacy notice[78] (itself hidden in very small print at the very bottom of the site) to get information about this right, or try to find it through the 'Help & Customer Service' section.[79] After several click-throughs and drop down menus with multiple choices people are finally led to a way to request 'all your data' via email.

In response to access requests by volunteers, the access volunteers did not feel that Amazon EU supplied all the data which it is likely to hold.

However, on the positive side, the process for Amazon EU's request for data via email is done directly from the customer's account and the company responds promptly. It requested a second input of the password to avoid fraud and providing the data within the prescribed period of 30 days.



**Amazon EU experience**

One volunteer asked Amazon UK "*if that is all the data Amazon processes about me and that I am entitled to under the GDPR?*". Amazon UK replied, "*We have reviewed your request and we are happy to confirm that we have completed your data subject access request. We have provided you with all the data that we store on you in line with the timeline determined by the GDPR legislation.*" Amazon EU's reply implies the company is not correctly interpreting and applying their obligation under the GDPR to provide a copy of personal data undergoing processing rather than merely data that they 'store on' individuals.[80]

On the question of how easy it was to exercise the right of access, one volunteer in Belgium commented that it was "*Not so easy. Information [in the privacy notice] pointed you to two different places to exercise your rights (without specifying where to go for the right of access).*" Two UK based volunteers also commented that Amazon EU supplied part of their personal data as a long list of codes that was unintelligible and not explained.

78. Amazon website, www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=201909010&ref_=footer_privacy#GUID-A440AA65-7F7E-4134-8FA8-842156F43EEE__SECTION_392EAF4C83FD47A2A360EF81917F7FBE see 'What Choices Do I Have?' after 504 words, individuals are advised they "have the right to request access to" their personal data and that if they *"wish to do [so], please contact Customer Service."*

79. Amazon website, www.amazon.co.uk/gp/help/customer/display.html/ref=hp_bc_nav?ie=UTF8&nodeId=201908990

80. Article 15(3) of the GDPR

### 3.5.2 Netflix EU/US: Proof of identity acts as barrier to data access

Like Amazon, our research found that Netflix at first appears to drive customers to only accessing data immediately available[81] at the account level and overall does not make it easy to exercise this essential right.

In terms of signposting, the privacy statement says to contact the company's Data Protection Officer/Privacy Office to make a request by email, but does not direct customers to the process that must be followed, which is listed ninth among the options set out on the Privacy and Security Help Page.[82] See Image 6.

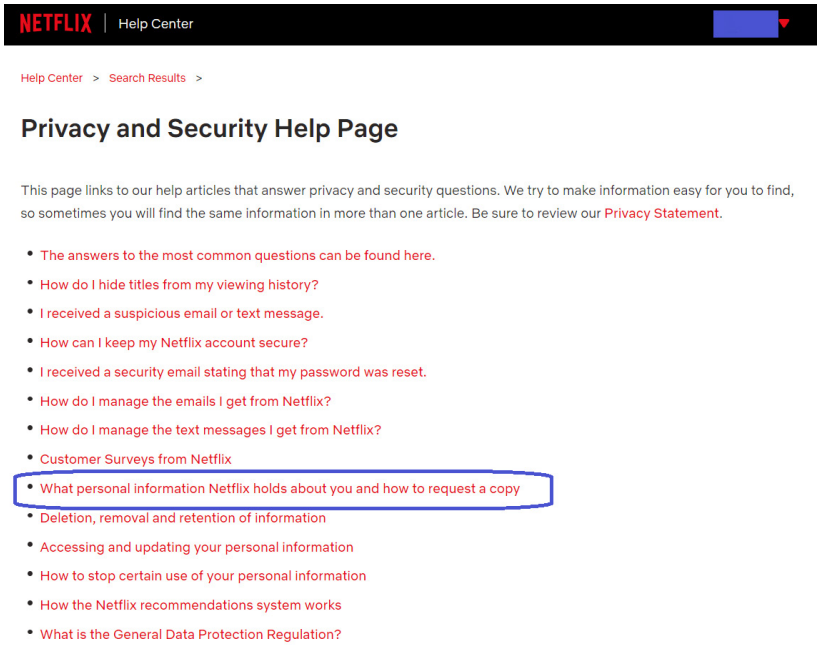



***Image 6: Netflix EU Privacy and Security Help Page***

#### Netflix experience

Two access volunteers based in Belgium, commented that the right to *"get a copy of the data is not explicitly mentioned (or at least I did not see that anywhere)… and it is not obvious how to find the right information."* One volunteer also felt that the text in the privacy statement was a "*mix of legalistic and simple language, but mostly legalistic*." They also commented that they "*had to send an email*" to request their personal data, and that while it was "*not difficult, an automatic tool to request access via a link on their site would have been easier*." The volunteer felt that "*from a company like Netflix I was expecting an automated way to request access, provided to the users in the 'my account' section.*" This is the process followed by Amazon EU and Spotify EU.

Netflix EU also refused to process the request of one access volunteer. The individual made the request from the email account registered on opening a Netflix account, and provided Netflix with the last four digits of a prepaid debit card, plus mobile number registered at the time of opening the Netflix account. Netflix EU insisted on government issued proof of identity. Netflix does not describe what it considers an "*official government issued ID document*" to be. The access volunteer asked Netflix *"why it is necessary to provide official government issued ID that I was not required to provide to Netflix when opening the account?"* Netflix replied after six weeks and insisted on government issued proof of ID revealing name, date of birth and country.

Similarly, one of the US – based volunteers was frustrated in the request for access to her personal data from Netflix because she did not want to share official government ID with the company.

81. Netflix website, https://help.netflix.com/en/node/100624 The privacy statement advises that *"…You can most easily do this by visiting the "Account" portion of our website, where you have the ability to access and update a broad range of information about your account"*
82. Netflix website, https://help.netflix.com/en/node/100628?ba=SwiftypeResultClick&q=privacy

The EU-based access volunteers found that Netflix requires proof of identity in the form of an official government-issued ID document (see box for volunteer experiences). This raises a number of important issues. Netflix allows people to create accounts without confirming their identity and date of birth, it accepts prepaid debit cards as payment, and people can set up a Netflix account using a pseudonymous identity. Why then is a government ID necessary for individuals to get access to their data? This demand may breach the GDPR. Rather than a blanket approach, the GDPR says that where an organisation has reasonable doubts about an individual's identity, it may request additional information necessary to confirm that person's identity.[83] The identification of individuals is important in protecting personal data against unauthorised disclosures, the identification requirements and process should be proportionate and not act as a barrier to such an important right.[84]

Under the CCPA a business such as Netflix is required to reasonably verify an individual. It can do this by associating information supplied by the customer with information it holds about the customer. The CCPA does not provide clarity on how a business should verify the identity of an individual requesting access to their data. It will be important for the California Attorney General to provide such clarity if identity verification is not to act as a barrier to the right of access.


83. Under Article 11(2) of the GDPR a controller must be able to demonstrate that it cannot identify the data subject, in order to refuse access. Under Article 12(6) where the controller has reasonable doubts about the identity of the individual making the request it may request additional information necessary to confirm the identity of the individual.

84. Recital 63 of the GDPR says that individuals should be able to exercise the right of access easily and at reasonable intervals.

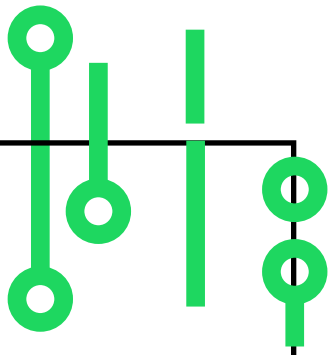
### 3.5.3 Spotify EU/US: Is this really all the data you have on me?

Spotify was found to only set out the right to obtain a copy of data under the right to portability[85] and did not clearly explain the separate and distinct right to obtain a copy of the personal data undergoing processing, as required by the GDPR.

The research suggests that Spotify's processes are designed to direct people to access their data via their accounts or to download their data from within their accounts via Spotify's download tool.[86]

However, Spotify was not found to describe what process a person should follow if they would like data not available via the download tool but which Spotify nonetheless processes. In the download your data section Spotify advises *"If you have any questions or concerns about the personal data contained in your downloadable file, please contact us,"* but this sends you back to downloadable only data. [87]

Spotify's help page for 'GDPR Article 15 Information'[88] says "*Your privacy and the security of your personal data is, and will always be, enormously important to us. Below you will find the information Spotify is required to provide about its processing of your data, under Article 15 of the GDPR.*" However, the Article 15 right to supplemental information cannot be entirely satisfied by a pre-published list of generic terms. Under this Article, individuals are entitled to receive the supplemental information in relation to the specific personal data undergoing processing. For example, they have the right to receive information about the sources of personal data not obtained directly from the individual, the third-party recipients to whom personal data is disclosed, joint data controllers, the purposes of processing of any joint controllership, the period for which personal data is retained, and the existence of profiling or automated decision-making.[89]



**Spotify experience**

Volunteers who made access requests to Spotify and who received copies of personal data do not believe that the data they received back was all the data held about them. One access volunteer asked Spotify via chat about the download tool and whether it supplied all the data that people are entitled to:

**Volunteer:** Will it provide everything that I'm entitled to under data protection law?

**Spotify agent:** Yup. If you would also like to receive the technical log information we collect to provide and troubleshoot the Spotify service, extended streaming history, or have a special data request, please let us know.

**Volunteer:** Isn't that included? Do I have to ask for it separately?

**Spotify agent:** This is because we only provide data collected from the last 180 days as per data regulations. If you want more info further than that, I can help you with it.

An EU volunteer sent a request for the additional information, which included enquiries about the advertising tracking conducted by third parties, and questions about the mobile app of Spotify. These requests have been outstanding since 23/24 September 2019 up until 6 December 2019.

85. Spotify website, www.spotify.com/uk/legal/privacy-policy/
86. ibid
87. The contact us link on the Spotify website takes you to www.support.spotify.com/uk/contact-spotify-privacy/
88. www.support.spotify.com/uk/account_payment_help/privacy/gdpr-article-15-information/
89. See footnote 44. In these guidelines on 'transparency' under the GDPR, EU data protection regulators have stated that by default, controllers should name precise recipients and not just "categories" of recipients. If they do choose to name categories, they must justify why this is fair, and be specific, naming "the type of recipient (ie by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.

The personal data supplied by Spotify EU to the access volunteers does not appear to contain all the categories of personal data variously set out by Spotify in its privacy-related notices, and to which people are entitled to under the GDPR. For example, no profiling data was supplied to any of the volunteers making requests, nor was data obtained by the companies from third parties.

The findings and concerns raised in this section are similar to those of the Austrian non-governmental organisation (NGO) NOYB,[90] which filed complaints in January 2019 with EU data protection authorities detailing the failures of Amazon Prime, Netflix and Spotify to comply fully with their obligations under the GDPR on the right of access.

**To conclude**, while the research showed that all the companies except for Amazon US tell people they have a right of access, they do not do so in ways that are always obvious or that make it easy to obtain a copy of one's personal data. The three companies investigated tended to direct access volunteers to data that is held at an account level or that is immediately available to the company, and do not explain, in accessible terms, the process to follow to obtain all of the personal data to which individuals are entitled under EU law. This requires regulatory scrutiny and enforcement action. Finally, the companies do not appear to provide all the personal data undergoing processing such as advertising profiles and related data. Under the CCPA, covered entities will be required to provide a copy of the specific information collected; it is unclear at this stage the degree to which that will apply to the personal information undergoing processing rather than 'collection'.

**Recommendations - right of access to personal data:**

- Companies should clearly signpost the information about the right to obtain a copy of all processed personal data and provide that information in a clear and simple form. The number of steps needed to request data should be kept to a minimum.
- Companies should find a right balance between the verifying individuals' identity to avoid fraud and making it easy for individuals to access their personal data, without demanding excessive extra personal data. Guidelines from authorities and common authentication standards are needed.

90. NOYB website, www.noyb.eu/access_streaming/

## 3.6 Data retention: How long is my data stored?

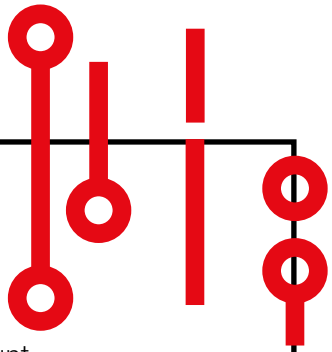
Data protection laws around the world, including the GDPR, prohibit organisations from keeping personal data longer than is needed for a lawful purpose. Organisations must justify their retention of personal data. To strengthen the transparent and fair processing of personal data, the GDPR requires organisations to tell people how long their personal data will be stored. The CCPA does not contain any similar prohibition or requirement to only collect and use the minimum data necessary for a specified purpose.

Based on the research, none of the investigated companies appear to comply with the obligation to set out the "*period for which … personal data will be retained*."[91] All three are ambiguous and use generic statements to the effect that they may keep data for as long as it is required or permitted by law. They variously invoke continued use of services, tax or accounting purposes, billing or records and fulfilling 'purposes described' in their privacy notices.[92] None of the companies specify the periods for which they will keep personal data, either by purpose of categories of personal data.

Successful access requests made to Amazon EU, Netflix EU/US, Spotify EU/US for copies of access volunteers' personal data revealed that the companies may keep certain behavioural data from the moment an individual opens an account (see Netflix experience box, below). Spotify, for example, clearly states in its privacy notice that it will retain the personal data *"for as long as you are a user of the Spotify. For example, we keep your playlists, song library, and account information."*[93]

Retention practices such as this enable the companies to tap into rich streams of their customers' behavioural data for many years. According to EU data protection authorities *"It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving period"*.[94]

In contrast to its EU counterpart, Amazon US' privacy notice was found not to mention data retention at all.



**Netflix experience**

Netflix supplied data to an access volunteer in Belgium that amounted to 446 pages of a pdf document that was difficult to read and understand.That data included detailed behavioural information generated and held since the volunteer opened their account in 2015, and was supplied for each individual who the account holder had created a profile for. The data included information about the titles of all content viewed, the country from which it was viewed, the precise data and time the content was viewed, the kind of device content was viewed from, how long the content was viewed and other data. This is extremely intimate data revealing important insights into a person's interests, tastes and behaviour. Netflix's privacy statement does not explain whether or how this data is used to support the activities of Netflix research.[95] It conducts research into how the company can predict consumer behaviour in order to support personalisation and experimentation into causal inference to measure new marketing and advertising ideas, for example.[96] The Netflix research activities require lots of data. An access request by a UK-based academic and policy researcher on another occasion revealed that Netflix captured and saved every choice made by individuals when watching the Black Mirror's Bandersnatch episode, which allowed viewers to choose different storyline endings[97]

91. Article 13(2)(a) and Article 15(1)(d) of the GDPR
92. Amazon website, Netflix website, www.help.netflix.com/legal/privacy and Spotify website,
93. Spotify website, www.spotify.com/uk/legal/privacy-policy/#s
94. See footnote 44
95. Netflix website, www.research.netflix.com/
96. Recent Trends in Personalization: A Netflix Perspective, Slide Share, 16/06/2019, www.slideshare.net/justinbasilico/recent-trends-in-personalization-a-netflix-perspective
97. Netflix Has Saved Every Choice You've Ever Made in 'Black Mirror: Bandersnatch', Vice, 12/02/2019 www.vice.com/en_us/article/j57gkk/netflix-has-saved-every-choice-youve-ever-made-in-black-mirror-bandersnatch

**To conclude**, it is impossible to determine the specific purposes the companies retain personal data for or the legal basis they rely on under the GDPR. This neither meets the requirements of the GDPR nor does it help individuals understand any risks and consequences for them. It also may undermine their ability to exercise their legal right to delete their personal data or to restrict its use. For example, where the retention supports profiling and interest-based advertising.

**Recommendations – data retention**:

- Companies should consider setting out in table format the retention period for each category of personal data, the purposes for keeping the data and the lawful basis.
- Companies should link to a clear explanation of rights that apply, and how an individual can easily exercise such rights, particularly the right to delete data. From a consumer perspective, this is particularly important for personal data that is kept for many years and reveals behaviours and habits, such as for example viewing data.

## 3.7 Android mobile app observations

Each company offers apps on the Apple and Google Android mobile platforms. Using the Exodus Privacy tool[98] the researcher and mystery shoppers in the EU and the US reviewed the Android app for each company. Each app contains a range of code (trackers) embedded in the app that fulfil a number of functions. These include reporting on the stability of the app and capturing data on user behaviour for first-party and third-party advertising purposes.

Like the main services, the apps are subject to the transparency and other obligations under the ePD and GDPR. In California they would also be subject to the CCPA and recommendations on mobile app privacy issued by the California Attorney General.[99] In the EU, embedding trackers in an app for purposes such as behavioural advertising requires the opt-in consent of individuals, as described in an earlier section of the report.

Only the Netflix app was found not to have any behavioural advertising trackers embedded. The Amazon Android shopping app[100] (see Image 7 below) contained the embedded advertising trackers Amazon Advertising and Google Ads. The mystery shoppers were not made aware of these trackers nor asked for consent. The research did not examine what data if any, the embedded trackers communicated to Amazon or third parties.

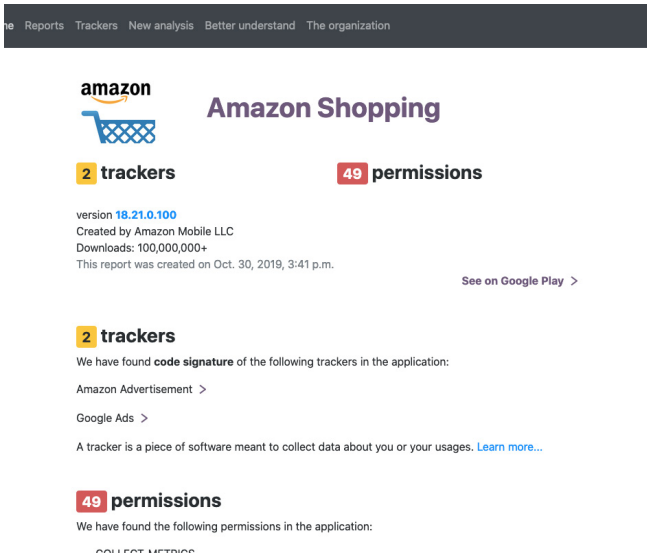



***Image 7: Amazon Shopping App Google play store***

98. Exodus website, wwwreports.exodus-privacy.eu.org/en/
99. Kamala D. Harris, Attorney General, California Department of Justice, Privacy on the Go: Recommendations for the Mobile Ecosystem, January 2013, www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf
100. Google Play website, https://play.google.com/store/apps/details?id=com.amazon.mShop.android.shopping&hl=en_GB

The Spotify Android app was found to be the most intrusive from a privacy perspective. It contained 10 embedded trackers, some of which support behavioural advertising, including Google Ads, Google Doubleclick, and Moat, and also trackers such as Facebook Analytics (image 8 below). This tracking happens without the required transparency and user consent under the ePD and the GDPR. The research did not examine what data the embedded trackers sent, if any, to Spotify or to the third parties. Regarding the latter, it is worth noting that Privacy International investigated the use of the Facebook tracker in 2018 and again in 2019 and its research found that Spotify automatically sent information to Facebook when its app was opened. As a result of those findings, Spotify notified Privacy International that it had "*updated the Spotify Android app to address the issues raised.*"[101]

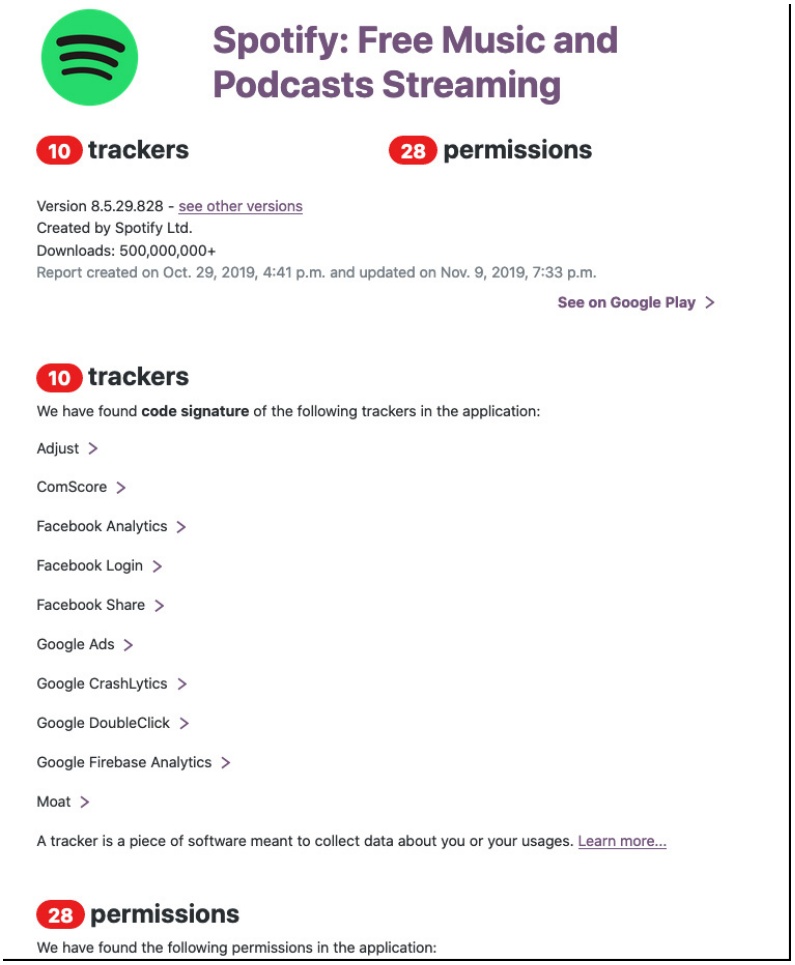
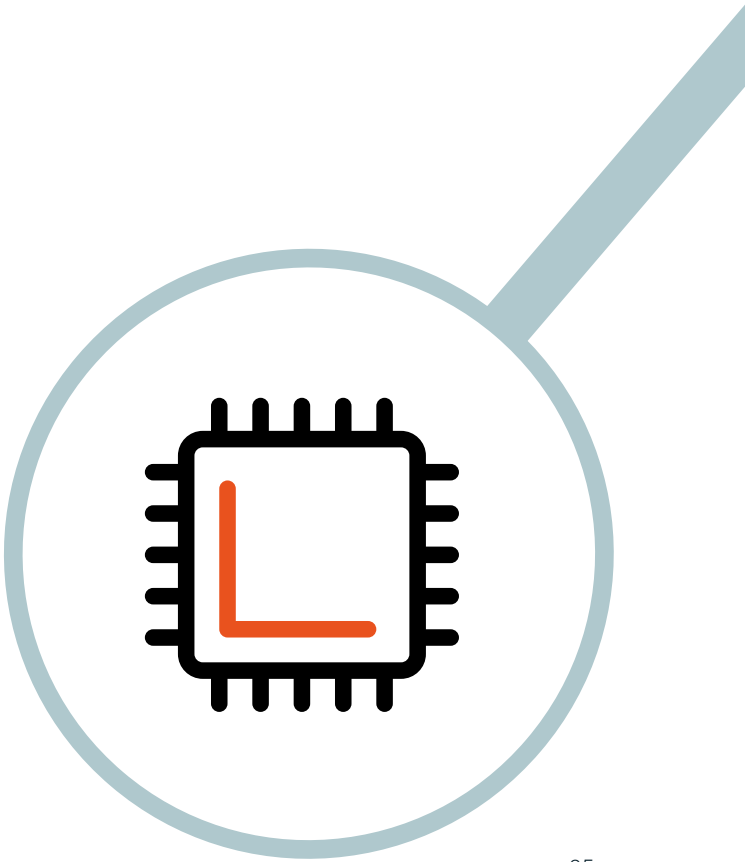



***Image 8: Spotify Free Music app, Google Play Store***



101. Privacy International website, www.privacyinternational.org/node/2498

Based on the findings of this research, Amazon EU and Spotify EU do not request nor obtain consent as required under the ePD for embedding trackers in their apps for the purpose of behavioural advertising. The companies also fail to meet their obligations under the GDPR to be transparent and clearly communicate information about the purposes and legal basis for processing personal data and about the right individuals have. The subsequent profiling and use of data for behavioural advertising must have a lawful basis under the GDPR. It remains unclear what legal basis Spotify EU and Amazon EU are relying on.[102]

A study carried out in 2017 analysed 180 mobile apps to understand the degree to which their privacy policies met guidelines on app privacy issued by the California Attorney General's Office in 2014.[103] The research found that the privacy policies were "*far from simplistic, with most requiring a minimum of a high-school diploma and some requiring at least a university degree*."

In January 2019, the French data protection authority imposed a fine of Euro 50 million on Google for failing to meet key transparency obligations when users configured their Android devices and created Google accounts. Google allegedly failed to provide privacy notices in an easily accessible form, using clear and plain language. Google also failed to obtain consent to process personal data for the purposes of ad personalisation. This regulatory action followed a complaint made by the NOYB.[104]

**To conclude**, Spotify and Amazon were both found to use code in their Android mobile apps to track users' behaviour for interest-based advertising. The code also appears to support third-party tracking. This tracking, especially by third parties, is not drawn to individuals' attention nor is their consent obtained when downloading or installing the apps. It is hidden from plain view. Individuals have no choice if they wish to use the apps.

The failure to be transparent and obtain consent also appears to breach Google's developer guidelines and terms[105] (Google is the owner of the Android mobile operating system). Additionally, the use of the Google Ads tracker by Amazon and Spotify breaches separate EU guidance,[106] which advises that "*You must be transparent in how you handle user data (eg, information collected from or about a user, including device information). That means disclosing the collection, use, and sharing of the data, and limiting the use of the data to the purposes disclosed, and the consent provided by the user*." Amazon and Spotify do not appear to meet these requirements.

**Recommendations – Android apps**:

- Amazon and Spotify should review their app practices and aim to comply with applicable law. Communication to users on mobile phone small screens is a particular challenge, but it is possible to do when they download and register for an app by providing immediate and easy links to the relevant settings and ensuring those are set to privacy by default.
- Google should provide an easy means for individuals to report concerns over an app's privacy practices.
- EU data protection regulators should conduct a review of the state of mobile app privacy and enforce applicable laws

102. Borgesius, F.J.Z., Personal data processing for behavioural targeting: which legal basis?, 23/06/2015, www.academic.oup.com/idpl/article/5/3/163/730611
103. Prichard et al, 'An analysis of app privacy statements', 2017, www.iacis.org/iis/2017/4_iis_2017_179-188.pdf
104. NOYB website, www.noyb.eu/news-update/
105. Google Play store website, www.play.google.com/about/privacy-security-deception/ and Google Play Developer website, www.developer.android.com/distribute/best-practices/develop/understand-play-policies
106. Google Ad Mob website, www.developers.google.com/admob/android/eu-consent#update_consent_status

# 4. CONCLUSIONS AND RECOMMENDATIONS

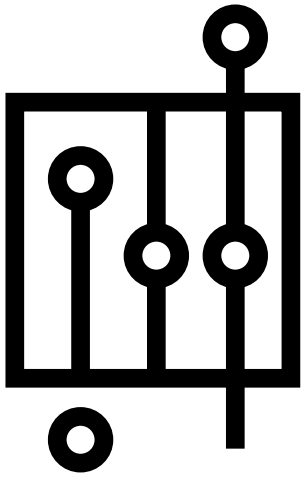
## RECOMMENDATIONS

Two key objectives of the GDPR are to strengthen the rights of individuals over the use of their personal data and strengthen the obligation on 'data controllers' such as Amazon, Netflix and Spotify to ensure their collection and use of personal data is transparent, fair and lawful. Other objectives include requiring controllers to build data protection by design and default into business practices and processing activities, and to require controllers to be accountable for ensuring compliance. While there is evidence that the GDPR has been a "*catalyst for a major overhaul of privacy policies inside and outside the EU,*"[107] it is unclear if that has improved the clarity of companies' policies and made exercising rights easier for individuals.

The research findings show much progress still needs to be made to provide individuals with key information about the use of their personal data and their rights, in concise, transparent, intelligible and easily accessible forms, using clear and plain language. The report also details how far companies still have to go to meet their obligations on matters of consent, online tracking, dark patterns and making it easy to exercise rights. The findings also suggest that consumer and privacy organisations need to continue researching and bringing cases before regulatory authorities and the courts, to ensure that rights are honoured and protected. This is only possible to a limited extent in the US, as there is currently no general privacy law and no data protection authority to complain to.[108]

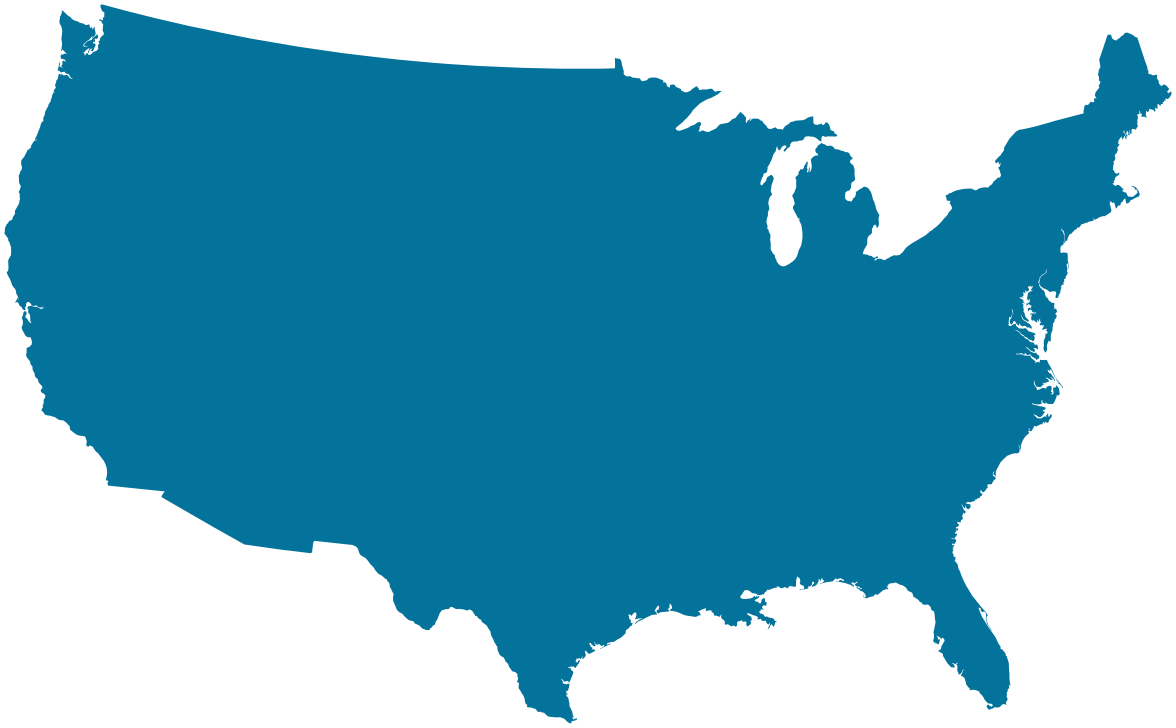
The CCPA obliges companies to communicate information to individuals about the source, use and sharing of personal data and key rights such as opting out of sharing data with third parties, accessing one's data, and deleting one's data. This information must be provided using plain, straightforward language while avoiding technical or legal jargon. This will require effective regulation and clear guidance that addresses the issue of readability and intelligibility of privacy notices, especially with regards to online tracking, which is invisible to individuals. A challenge of such regulation, as with the GDPR, is to match the promise of better privacy with accountability and enforcement.

Based on our research, it appears that much progress still needs to be made by the companies investigated towards ensuring their use of personal data is transparent and enabling individuals to exercise their rights effectively.



107. Linden et al, The Privacy Policy Landscape After the GDPR, 22/09/2018, www.arxiv.org/abs/1809.08396

108. The enforcement statutory powers of the FTC in the area of privacy are limited to unfair or deceptive acts or practices (section 5 of the FTC Act). For example, deceitful practices such as dark patterns would be covered by FTC, but not any other privacy infringement.



## RECOMMENDATIONS TO THE US

This research contributes to the existing evidence that a comprehensive and meaningful privacy protection in the US is needed.[109] We recommend that:

- States should enact strong privacy legislation.
- Congress should enact a baseline privacy law that does not pre-empt stronger state privacy protections and establishes an independent data protection agency responsible for overseeing and enforcing it.
- Privacy legislation should include provisions to:
    - Federal privacy legislation should establish an independent data protection authority that is appropriately empowered and resourced
    - Require transparency about data practices
    - Require data minimisation
    - Protect civil rights
    - Limit data retention
    - Require data accuracy
    - Require data security
    - Give individual rights of access, correction and deletion
    - Prohibit dark patterns and other manipulative practices
    - Require privacy by design and default
    - Hold data controllers accountable
    - Give individuals private rights of action, providing meaningful redress and statutory damages
    - Give government agencies strong enforcement powers
- Federal privacy legislation should establish an independent data protection authority that is appropriately empowered and resourced.[110]

109. TACD, GDPR - 10 things you need to know (US perspective), May 2018 www.tacd.org/wp-content/uploads/2018/05/GDPR-US-10-things-you-need-to-know-052018_final.pdf See also US NGOs, including several TACD members, The Time is Now: Recommendations on a framework for comprehensive privacy protection and digital rights in the United States, January 2019,

110. European Union Agency for Fundamental Rights, Elements of independence of the data protection authorities in the EU Data protection authorities' funding and staffing, www.asktheeu.org/en/request/2398/response/9765/attach/3/21.FRA%20Focus%20Data%20protec-

## RECOMMENDATIONS TO THE EU

In the EU, regulators have issued guidance on transparency, consent, and online tracking and behavioural advertising, and are now considering guidance on individuals' rights.[111] However, based on our research, it appears there are still improvements to be made to business practice. Change will require enforcement by regulators and continued pressure and litigation from consumer and privacy organisations. We recommend that:

- Regulators co-ordinate globally to investigate companies' practices in relation to user controls over personal information, as was carried out by the Global Privacy Enforcement Network in 2017.[112] Consumer and privacy organisations could co-ordinate freedom of information requests on such activities to assist in holding regulators to account.
- Regulators develop guidance on the application of data protection by design to the protection and exercise of rights, especially the right of access.
- Regulators conduct reviews of the data practices of major organisations and encourage better transparency and compliance with the right to access, delete, and restrict the processing of personal data and other individual rights.
- Regulators encourage data protection by design and default and discourage use of dark patterns and other practices that prevent individuals from exercising their choices and legal rights. Regulators should issue clear guidance but also take robust enforcement action.
- Regulators develop guidance on what constitutes proof of identity in the context of making a request for a copy of personal data or the deletion of data. This remains an issue under the GDPR and is likely to be a key issue under the CCPA. It is important that proof of identity is not used as a barrier to the exercise of these rights.
- Consumer and privacy organisations continue to improve their technical capabilities and work with each other and with academic researchers to investigate the data practices of apps and services. Evidence from such practices is proving crucial in encouraging organisations to change their practices and regulators to act.[113]

tion%20authorities%20independence%20funding%20and%20staffing%20ATTACHMENT%20FRA%202013%20Focus%20DPA.pdf

111. EDPB Stakeholder Event on Data Subject Rights, www.edpb.europa.eu/news/news/2019/edpb-stakeholder-event-data-subject-rights_en

112. UK Information Commissioner's Office, GPEN Sweep 2017 'User Controls over Personal information', October 2017, October 2017, www.astrid-online.it/static/upload/2017/2017-gpen-sweep---international-report1.pdf

113. See footnote 22