الاستهداف السلوكي في المملكة العربية السعودية: الممارسة ومخاوف الخصوصية

مها عبدالعزيز المطلق*

DOI:10.15849/ZJJLS.240330.31

* **قسم القانون الخاص، كلية القانون، جامعة الأميرة نورة بنت عبدالرحمن، المملكة العربية السعودية .**

* للمراسلة: maalmutlak@pnu.edu.sa

الملخص

الاستهداف السلوكي هو مراقبة أنشطة الأفراد عبر الإنترنت وتجميع سجل لاهتماماتهم لإنشاء ملف تعريف وإرسال إعلانات مخصصة. يعد الاستهداف السلوكي نشاطًا تجاريًا سريع النمو على الإنترنت، مما يساعد شركات الإعلان على الوصول إلى جمهورها بشكل أسرع. يعد الاستهداف السلوكي انتهاكًا لخصوصية المستخدمين. في المملكة العربية السعودية، يمثل الوضع تحديًا كبيرًا، ويرجع ذلك أساسًا إلى العدد الكبير من مستخدمي الإنترنت وانتشار الاستهداف السلوكي. وتتفاقم هذه المشكلة بسبب غياب المحظورات القانونية في الإطار الحالي. وتنتشر هذه الممارسة بسبب غياب التشريعات الواضحة والفوائد الاقتصادية الكبيرة التي تعود على المعلنين. بعد وصف الاستهداف السلوكي، تقدم هذه الورقة خلفية عن مدى انتشار استخدام الإنترنت في المملكة العربية السعودية. ثم تناقش أهمية الاستهداف السلوكي. بعد ذلك، تقوم هذه الورقة بتحليل القوانين ذات الصلة وتقييم جذور المشكلة، واقتراح توصيات لضمان الخصوصية على الإنترنت في المملكة العربية السعودية.

الكلمات الدالة: الاستهداف السلوكي، مقدمو خدمات الإنترنت، مستخدمو الإنترنت، الخصوصية، التتبع.

Behavioural Targeting in Saudi Arabia: Practice and Privacy Concerns

Maha Abdulaziz Almutlak*

***Department of private law , College of Law, Princess Nourah Bint Abdulrahman University, Saudi Arabia**

*** Crossponding author:** maalmutlak@pnu.edu.sa

Abstract

Behavioural targeting is monitoring individuals' online activities and compiling a record of their interests to create a profile and send customized advertisements. Behavioural targeting is a fast-growing business on the internet, helping advertising companies reach their audience faster. Behavioural targeting is an invasion of users' privacy. In Saudi Arabia, the situation presents a significant challenge, primarily due to the substantial number of internet users and the widespread of Behavioral targeting. This issue is further compounded by the absence of legal prohibitions within the current framework. The practice pervades because of the absence of clear legislation, and large economic benefits for advertisers. After describing behavioural targeting, this paper provides a background on the prevalence of internet usage in Saudi Arabia. This paper then discusses the significance of behavioural targeting. After that, this paper analyses relevant laws and assesses the root of the problem, suggesting recommendations ensuring online privacy in Saudi Arabia.

Keywords: behavioural targeting, internet service providers, internet users, privacy, tracking.

1. Statement of the Problem

Behavioral targeting is the monitoring of individuals' online activities and compiling a record of their interests over time to create a profile. It aims to send customized advertisements based on users' profiles, to increase purchasing power. It is considered in an invasion of privacy of internet users. In Saudi Arabia, the situation presents a significant challenge, primarily due to the substantial number of internet users and the widespread utilization of behavioral targeting. The practice pervades due to absence of clear legislation, and large economic benefits for advertisers.

2. Study Objectives

1- To point out that the practice of behavioural targeting is an invasion of privacy and therefore illegal.
2- To assess the societal awareness of the practice of behavioural targeting in Saudi Arabia.
3- To understand the legal landscape of privacy in Saudi Arabia.
4- To recommend suitable solutions and remedies to end the practice of behavioural targeting, and increase the privacy for internet users in Saudi Arabia.

3. Research Questions

1- What is Behavioural targeting, and what are the reasons for its wide spread utilization in Saudi Arabia?
2- Are the people of Saudi Arabia aware they are being monitored online, and do they understand the legal consequences for such monitoring?
3- Are the current legal framework in place insufficient in ending the practice?

4. Introduction

"Behavioural targeting", "online behavioural advertising", and "online profiling" are all synonyms referring to the same practice that includes monitoring an individual's online activities and compiling a record of the individual's interests over time to create a profile. According to Hotaling[1], Behavioural targeting aims to send customized and specific advertisements to these individuals based on their profiles, as it will probably increase the purchasing power of potential customers. Information about the individuals is usually gathered from the websites they visit and/or their search history. Even though the information collected to create the individual's profile does not necessarily contain personal information, such as name or address, Barbaro and Zeller[2] assert that the specificity and privacy of the collected data are so pronounced that the individuals can be identified through the information contained in the profile.

To illustrate what behavioural targeting is, consider when an individual searches for sunglasses online. The individual soon starts to receive ads with the same sunglasses when opening a new web page or via email. While some people are naïve enough to think it is a coincidence, the insidious issue is much deeper. This practice enables advertisers to identify and reach their

[1] Hotaling, A. (2008) 'Protecting Personally Identifying Information on the Internet: Notice and Consent in the Age of Behavioural Advertising', CommLaw Conspectus, Vol. 16, pp. 529–565, 530.

[2] Barbaro, M. and Zeller Jr., T. (2006) 'A Face is Exposed for AOL Searcher No. 4417749', New York Times [online] 9 August. https://www.nytimes.com/2006/08/09/technology/09aol.html

target audience faster. From a legal perspective, this is concerning as it is a clear violation of an individual's privacy, yet Boerman et al.[1] suggest that many individuals are not even aware of the practice and that their privacy is being breached. On the other hand, some individuals are aware but prefer behavioural targeting as it helps them get what they need.

Cookies are programs that are being used by different websites as tracking technology or software to monitor visitors. Esposito[2] notes that a cookie is a piece of data that a website sends to a web browser, requesting to retain the consumer's web browser, flash cookies and beacons. Websites use these tools to scan visitors' online movements and analyse other relevant information such as age, location, income, and shopping preferences and later sell this information to marketing companies. What adds to the concern is that even when an individual removes a website from their browsing history, Hoofnagle[3] reveals that these tools can persistently continue to track their information. Behavioural targeting is a booming business on the internet. In today's world, the internet has permeated people's lives using mobile phones, computers, and tablets. The prevalence of internet usage among the general population increases the need to protect privacy due to the ongoing and increasing threat of behavioural targeting. There is a growing global initiative to protect online data privacy, led by the General Data Protection Regulation (GDPR) in the EU. This demonstrates that online privacy is increasingly becoming a global issue that needs to be addressed.

Sprague and Ciocchetti[4] noted that everything an individual does online can be monitored and information stored on ISP servers. Sometimes, data about users can be sensitive or embarrassing but users are unable to control, protect or even monitor their data. Moreover, information collected about users can help identify users easily. This is harmful to users and Berger[5] notes that there is the possibility of data-related crimes that can include financial fraud and identity theft which is high because of user profiling where data can be disclosed unlawfully harming those individuals.

Additionally, internet users cannot assess the risk of losing their privacy through behavioural targeting. Users are not always aware their data is being traced and stored for advertising purposes. Berger[6] explained this clearly, noting that the average consumer or internet user is unable to comprehend the vague processes of behavioural targeting.

An overly critical point is obtaining prior approvals to conduct behavioural targeting by advertising companies and ISPs through privacy statements, which mention the use of personal data for advertising purposes or third-party sharing. Most people unintentionally accept data sharing for behavioural targeting through complex ISP privacy statements. According to

[1] Boerman, S. et al. (2017) 'Online Behavioural Advertising: A Literature Review and Research Agenda', *Journal of Advertising*, Vol. 46 No. 3, pp. 363–376, at 367.
[2] Esposito, D. (2006) *Programming Microsoft Asp.Net 2.0 538*, Pearson, Redmond.
[3] Hoofnagle, C.J. et al. (2012) 'Behavioural Advertising: The Offer You Cannot Refuse', *Harvard Law & Policy Review*, Vol. 6, pp. 273.

[4] Sprague, R. and Ciocchetti, C. (2009) 'Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws', *Albany Law Journal of Science & Technology*, Vol. 19 No. 1, pp. 91–140, 93 (discussing how consumers lose control over personally identifying information (PI) when they disclose it to businesses, and how businesses use PI for data mining).
[5] Berger, D. D. (2010) 'Balancing consumer privacy with Behavioural targeting', *Santa Clara Computer & High Technology Law Journal*, Vol. 27 No. 1, pp. 3–62.
[6] Berger, D. D. (2010) 'Balancing consumer privacy with Behavioural targeting', *Santa Clara Computer & High Technology Law Journal*, Vol. 27 No. 1, pp. 3–62.

Boerman et al.[1], What is worrisome, is that nobody reads privacy statements. And even when some *do* read the privacy statement, the complexity of the language prevents users from understanding the parameters of the agreement. This allows ISPs to claim transparency and user approval. However, users do not know what they are agreeing to. Although signing is required lack of understanding of privacy agreements prevents users from redressing the harm that might come from invading their privacy, such as the misuse or inappropriate disclosure of personal data. This also means that relevant privacy laws cannot apply in this situation can create a bigger dilemma for users. For transparency, users should be asked a clear and short (one-sentence) question about agreeing to share their data instead of incorporating this provision inside lengthy privacy statements.

The research paper is structured as follows. First, the background of behavioural targeting in Saudi Arabia is discussed. Following the background, this paper discusses the harms caused by behavioural targeting and the significance of these harms, hence, the importance of addressing the issue. Finally, this paper analyses relevant laws and assesses the root of the problem, suggesting suitable recommendations to ensure the privacy of consumers and online users in Saudi Arabia.

5. Saudi Arabia as Study Setting

The e-commerce market in Saudi Arabia is experiencing fast and rapid growth. According to Saudi Arabia and Social Media Statistics[2] 93% of the population in Saudi Arabia has internet access. The 2018 CIGI-Ipsos Global Survey on Internet Security and Trust[3] highlights the significant expansion of Saudi Arabia's e-commerce market, positioning it among the world's largest. Additionally, according to Santander trade profile[4], Saudi Arabia ranks at the top of active internet users within the entire MENA region on social networks with 89.39% active internet users, based on Saudi Arabia and Social Media Statistics[5].

Currently, Saudi Arabia has the most active social media users in the world (67.95% of the total population) with an average of 2 hours and 50 minutes of social media usage a day. For instance, 38% of Saudis use Snapchat daily, and Saudis comprise 9% of all Snapchat users. Crowd Analyzer[6] reported that Saudi Arabia has the world's largest number of monthly active Snapchat users, with 14.56 million users.

These numbers are tempting to advertisers who use behavioural targeting to reach their preferred audience and show little concern for user privacy. Therefore, as Alzahrani[7] notes, behavioural targeting is quite common in Saudi Arabia—especially in applications such as

[1] Boerman, S. et al. (2017) 'Online Behavioural Advertising: A Literature Review and Research Agenda', *Journal of Advertising*, Vol. 46 No. 3, pp. 363–376, at 367.

[2] *Saudi Arabia Social Media Statistics 2019*. [online] https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/ (29 October 2019).

[3] 2018 CIGI-Ipsos Global Survey on Internet Security and Trust. [online] https://www.cigionline.org/internet-survey-2018#:~:text=The%202018%20CIGI-Ipsos%20Global%20Survey%20on%20Internet%20Security,privacy%20and%20the%20power%20of%20social%20media%20platforms (Accessed 31 August 2020).

[4] *Saudi Arabia: Reaching the Consumer*. [online] https://santandertrade.com/en/portal/analyse-markets/saudi-arabia/reaching-the-consumers (Accessed 28 August 2020).

[5] *Saudi Arabia Social Media Statistics 2019*. [online] https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/ (29 October 2019).

[6] *The State of Social Media*. (2020) [online] https://www.crowdanalyzer.com/hubfs/Reports%202020/SOSM%20Report%2020_ENG_Final_May.pdf (Accessed 1 September 2020).

[7] Interview with Dr. DaifAllah Alzahrani (Deputy Governor for Competition and Legal Affairs at the Commission of Communication). (26 July 2020).

Snapchat and Instagram, which use certain tools that save users' information for marketing purposes. Behavioural targeting is growing rapidly as targeted ads are increasing noticeably from year to year. Advertising companies rely heavily on this form of marketing due to its success and increased revenue generation.

The Communications and Information Technology Commission (CITC) is the authority in Saudi Arabia responsible to monitor Internet communications. According to a member of the CITC, the Commission is aware of behavioural targeting. However, the commission has yet to actively address this issue as the cost of monitoring behavioural targeting is high. Moreover, low levels of complaints from users regarding behavioural targeting, primarily due to a lack of awareness of their rights, make this a secondary issue for the Commission. The need for legislation in Behavioural Targeting is further highlighted by the 2018 CIGI-Ipsos Global Survey on Internet Security and Trust[1] which noted that online privacy is a growing interest and concern to half of the internet users around the world, especially with growth of social media. This shows the importance of creating and enforcing legislation that protects the privacy of internet users to deal with such concerns.

6. Study Methodology

The paper analyses relevant laws and regulations in Saudi Arabia to assess the legal perspective of behavioural targeting within the Kingdom. While there are no laws that deal with behavioural targeting directly, privacy-related laws are analysed in this paper and linked to behavioural targeting. The study also bases its findings on a research questionnaire distributed to 297 Saudis, measuring societal awareness of the practice and the legal understanding of behavioural targeting. The survey was distributed online and targeted all strata of society (no educational level required). The survey demonstrated that many are unaware of the practice, are unaware that it is against the law, and frequently fail to thoroughly read privacy statements.

7. Issue Function and Significance

Behavioral targeting includes monitoring users' online activities, their browsing patterns and history by internet service providers (ISPs). The information is then utilized to deliver personalized advertisements. However, it's important to note that ISPs typically do not directly install software on users' computers or sell data to third-party companies for this purpose. Instead, behavioral targeting primarily relies on the collection of users' online behavior data, which is used by advertisers to create tailored advertisements. According to Albanesius[2], ISPs can use this data, either by selling it to third parties who then send customized ads, or by employing it to enhance their own advertising efforts.

Steps of the behavioural targeting network process:

- Companies that wish to market their products hire the services of advertising companies to establish infrastructure and to show ads on websites through their ad servers.
- Advertising companies may request space from website owners to display their ads on their websites.

[1] 2018 CIGI-Ipsos Global Survey on Internet Security and Trust. [online] https://www.cigionline.org/internet-survey-2018#:~:text=The%202018%20CIGI-Ipsos%20Global%20Survey%20on%20Internet%20Security,privacy%20and%20the%20power%20of%20social%20media%20platforms (Accessed 31 August 2020).

[2] Albanesius, C. (2008) 'Should Your ISP be allowed to Serve You Spyware?', *PC Magazine* [online] 28 April. http://www.pcmag.com/print article2/0,1217,a=226952,00.asp?hidPrint-true.

- While users navigate a website, the website can deliver advertisements to them. Upon clicking the advertisement, users' information is transmitted to the servers of advertising companies. Advertising companies then send cookies, which are initially stored on the website (until the browser is closed) and later permanently stored on the hard drive, keeping track of users' interests and searches.

Advertising companies employ data management tools to analyse users' behaviours and create patterns for future targeting. Users are further classified depending on their interests. Subsequently, advertising companies display relevant ads to the right audience.

7.1 Survey Data

The survey aimed to measure Saudi Arabian society's awareness of the practice of behavioural targeting and its legal implications. The respondents who participated in the survey were interested in the topic and excited to see scholarly work focused on practice and online privacy.

The results of the survey show that most people were not aware of the specific practice of behavioural targeting and did not know that this practice is a violation of privacy. While many survey participants noticed ads customized according to their online searches, they did not know that this meant their data was collected and saved on online servers. Participants of the survey were mostly aware that customized ads are not a coincidence, however, they were not concerned enough to learn how it happens. Most participants preferred customized ads since they suggested things that they like.

Most survey participants frequently failed to thoroughly read privacy statements, and many received ads without an opt-out opportunity. More than half of the participants confirmed that they continued to receive ads, even after opting out.

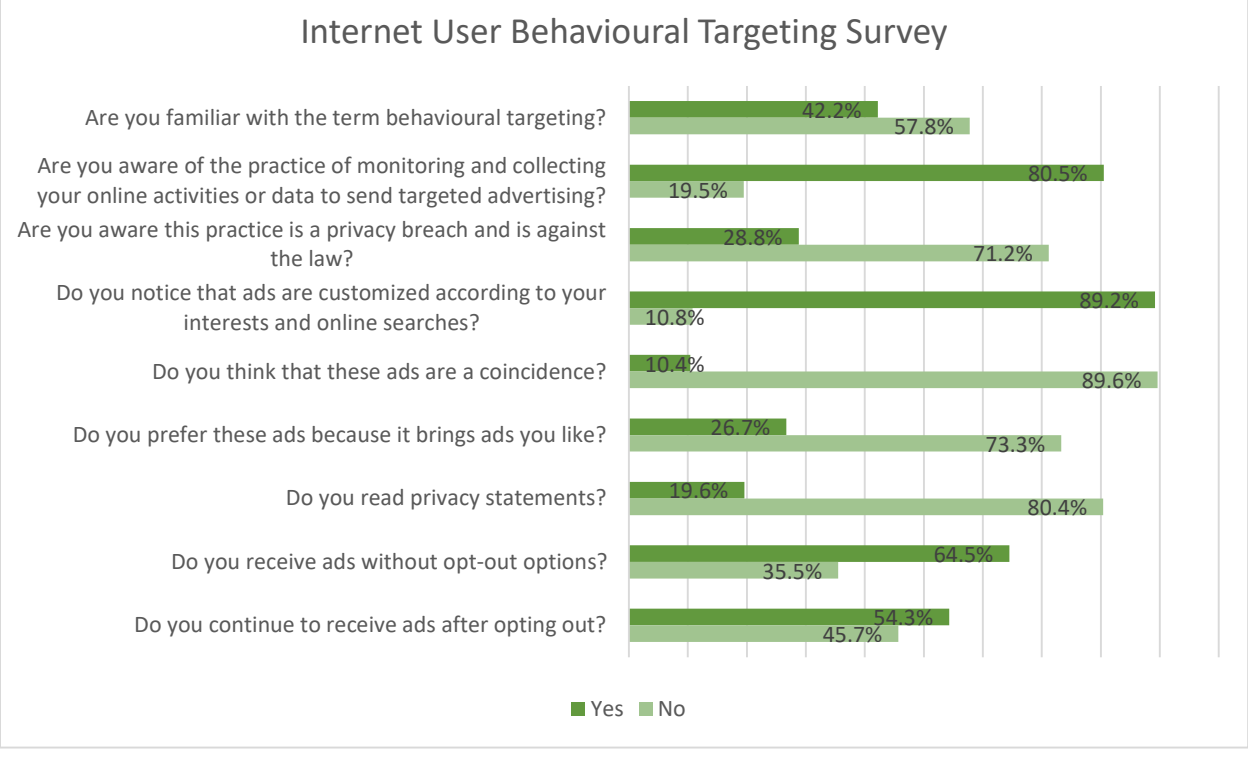

Figure 1. Survey Results

8. Analysis of Relevant Legal Framework

Even though the specific mention of the behavioural targeting act is not explicitly regulated by the law. This section links different laws and regulatory documents to behavioural targeting through the analysis of relevant codes. The purpose is to understand the legal landscape of data privacy and develop recommendations to improve legal protections for user privacy and prevent predatory behavioural targeting.

8.1 The Basic Law of Governance (Constitution) (1992)

Article 40 of the Saudi Basic Law of Governance[1] mentions that "telegraphic, postal, phone communications and any other forms of communication are protected by the law and are guaranteed privacy except in cases determined by the law".

Analysis

While Article 40 does not specifically mention data, it emphasizes the value of privacy protection for all forms of communication. This can, by analogy, include individual privacy through online activities as the purpose of this protection is the same.

8.2 The Executive Regulation of the Law of Communications (2018)

Article 58 of the Executive Regulation of the Law of Communications[2] discusses the protection of personal data, stating that ISPs are responsible for the personal data of users and all communications under their control. Under Article 58, ISPs must operate their systems and communications while considering the privacy of users and, unless permitted by the law or authorized by the user, ISPs must not disclose the personal data of users or their communications for any purpose whatsoever. Moreover, the purpose of collecting or compiling the personal data of users must be identified before or during the collecting and compiling process, and ISPs must not collect or compile data for any reason other than the disclosed purposes. Specifically, ISPs must not reveal any data collected or compiled and ISPs must make sure that the personal data of users is updated and precise to achieve the objectives of collecting and compiling this data. ISPs must ensure that personal data is protected with appropriate measures subject to the data's sensitivity.

Analysis

The regulation obligates ISPs to protect the personal information of users. It also prohibits ISPs from sharing the personal data of users for any purpose. Thus, even though behavioural targeting is not mentioned specifically, sharing information with any third party for advertising purposes is forbidden, which includes sharing with companies engaged in behavioural targeting. The regulation also mandates transparency, requiring ISPs to identify the reasons for collecting the data. Thus, if the data is collected for advertisement purposes, ISPs must seek the prior consent of users. ISPs are forbidden from revealing the personal data of users, which includes sharing or selling this data for advertising purposes.

8.3 The E-Commerce Law and the Executive Regulation of the E-Commerce Law (2019)

[1] Basic Law of Governance (1992). https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/16b97fcb-4833-4f66-8531-a9a700f161b6/1

[2] Ministerial Decision No. 53 (2018). [online] https://www.citc.gov.sa/ar/RulesandSystems/Bylaws/Pages/TelecomActBylaw.aspx.

Issued in 2019, the E-Commerce Law and its Executive Regulation[1] applies to the relationship between ISPs and consumers involving transactions in Saudi Arabia. Article 5(1) states that ISPs cannot save consumers' personal information or consumers' communications except for the time needed to conduct the transaction (time retention). ISPs are also obligated to take measures to ensure the safety and privacy of consumers' data while the data is under the control of the ISPs or the control of third parties interacting with the ISPs.

Article 5(2) states that ISPs cannot use consumers' data or personal communications for unauthorized use or share this data with third parties without prior consent from the consumer unless otherwise stated by the law.

The Executive Regulation of the E-Commerce Law was issued shortly after the E-Commerce Law with the intent to explain the articles of the law in more detail. Article 5(1) of the Executive Regulation explains that the personal data mentioned in Article 5 of the E-Commerce Law includes any identifying consumer information such as name, identification number, address, telephone numbers, numbers of permits, personal properties, bank information, and pictures.

Under Section 2 of Article 5 of the Executive Regulation, ISPs are obligated:

- To apply administrative and technical measures to protect the personal data of consumers from being reached, released, exchanged, or processed for unauthorized purposes.
- To not retain data longer than required for the transaction and to not use the data for any other purposes, such as marketing or advertising, without express consumer consent.
- To notify the Ministry of Commerce and the consumer within three days of learning that a consumer’s data has been compromised, specifying the range of the penetration, its consequences, and the necessary measures taken to resolve the penetration.
- To store consumers' data with consumer consent if the relationship between the ISP and the consumer is a continuous relationship, which requires creating a profile or account for the consumer to facilitate future transactions, provided the consumer can easily ask the ISP to remove this account at any time.

Analysis

These articles intend to protect the personal data of consumers that is defined by the Executive Regulation as name, identification number, address, etc. under the control of the ISP. Control refers to the ability of the ISP to make decisions concerning the data, including the reason for the collection of data, length of storing the data, and third-party sharing of data.

The articles do not explicitly forbid behavioural targeting; however, Article 5 of the Law mentions the protection of consumers’ communications, which can include activities conducted on the website. Additionally, the referenced articles of the E-Commerce Law demonstrate the legislature’s intent to protect the consumers. This is illustrated in the prohibition of third-party sharing without prior consent from the consumer.

Article 5(1) of the Executive Regulation explains protected personal data as “any information that leads to identifying the consumer”. The language used in the article could refer to behavioural targeting. Even though it does not specifically mention this practice, the creation of profiles by ISPs, which aim to send specific advertisements to these consumers can help identify consumers. Also, the explanations of protected personal information referenced in Article 5(1) were mentioned as examples and not exclusively.

[1] Royal Decree No. M/126 (2019). [online] https://mc.gov.sa/ar/ECC/Pages/default.aspx.

"Any other uses" of personal consumer data, as mentioned in Article 5(2)(B), can include the practice of behavioural targeting especially since the legislature used advertising and marketing as examples to show the necessity of obtaining consent for such causes.

8.4 Reduction of Spam Regulatory Document (2018)

The Reduction of Spam regulatory document[1] was issued by the CITC in 2018 with the intent to reduce the amount of electronic spam messages internet users received. Spam messages are defined in this document as electronic messages that do not have an opt-out option. This document classifies the types of messages as cautionary messages, awareness messages, service messages, personal messages, and advertisement messages.

The regulatory document explains the guidelines for sending advertising messages in point number three:

- The message should contain the sender's electronic address (such as email);
- The user must be able to opt out of clearly and easily receiving more messages.
- The sender must stop sending messages within 24 hours of receiving the opt-out request.
- The sender must send a notification confirming the receipt of the opt-out request.
- The sender must not use Flash SMS.
- The sender may not use programs to collect addresses or use emails or electronic addresses obtained through these programs.
- The sender may not send spam messages.

Analysis

Advertisement emails received by the users including emails sent as part of behavioural targeting do not always provide for a clear opt-out option; when they do, they sometimes do not adhere to the opt-out after receiving the request. This is a violation of the above-mentioned code, thus, these advertisement emails are considered spam messages.

8.5 Electronic Transactions Law (2007)

The Electronic Transactions Law[2] aims to regulate and control electronic transactions. Article 2 of the law:

- Sets standardized regulations for electronic transactions, which can be easily applied for both the public and private sectors.
- Promotes confidence in the validity of electronic transactions.
- Facilitates the use of electronic transactions both locally and internationally to benefit all fields, such as governmental procedures, business, medicine, education, and electronic financial payment.
- Removes barriers to the use of electronic transactions.
- Forbids misuse and fraud in electronic transactions.

[1] Reduction of Spam Regulatory Document (2018). [online] https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT010A_Regulation_For_The_Reduction_of_SPAM_Ar.pdf.
[2] Royal Decree No. M/18 (2007). [online] https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_003_%20A_E-Transactions%20Act.pdf

Article 3 applies the law to electronic transactions. According to Article 1, electronic transactions are "any exchange, correspondence, contract, or any other procedure that is concluded full or partial by electronic means".

Analysis

Advertisements, whether website ads or emails that are sent to users based on user profiling and tailored to user preferences fit in this category. According to Article 3, they are correspondence sent electronically. By sending tailored ads electronically, ISPs are violating Article 2 of the Electronic Transactions Law. Specifically, these ads violate the trust and confidence that aims to embed in electronic transactions. Sending tailored advertisements raises questions about trusting ISPs that are tracking and compiling this data, often without the explicit knowledge of users. Additionally, violating the privacy of users by using their information and data to send customized ads is considered a misuse of electronic transactions, also forbidden by Article 2.

Although this law does not mention behavioural targeting per se, it still forbids acts leading to behavioural targeting. Thus, this part of the legal framework can be relied upon to prevent ISPs from targeting users through behavioural targeting.

8.6 The General Rules to Protect the Privacy of User's Data in the Telecommunications, Information Technology, and Postal Sectors (2020)

The General Rules to Protect the Privacy of User's Data in the Telecommunications, Information Technology, and Postal Sectors[1] document aims to ensure the privacy of users' data and to protect their rights according to the recommended international practices. It also aims to enhance trust in these different communication services, which depend on processing the personal data of users.

Personal data in this document is defined as "any data regardless of source or nature which can lead to identifying a user precisely or making a user identifiable directly or indirectly. This includes but is not exclusive to names, identification numbers, addresses, communication numbers, permit numbers, personal properties, bank information and pictures, and any other data with a personal character". Data leakage here is defined as "disclosure, revelation, publication, or allowing access to personal data without legal basis, intentionally or unintentionally".

Section 2 states that "the processing of personal data should be done for specific purposes that are clear to the user", while Section 3 recognizes that "collection of data should be minimal and only to meet the purpose of collecting the data". Section 4 of the document discusses the basic guidelines for protecting the personal data of users, stating "ISPs must not retain data in a format that allows identification longer than required—only for collection". Section 5 states that "ISPs must protect the personal data of users by ensuring its privacy, prohibiting unlawful access to it, leaking it, or misusing it".

Analysis

The definition of personal data is identical to the definition from the Executive Regulation of the E-Commerce Law. The definition encompasses a wide range of data, including online activities, since an individual's online Behaviour can readily assist in identifying the user.

[1] Data Privacy Principles for ICT (2020). [online] https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT010A_Regulation_For_The_Reduction_of_SPAM_Ar.pdf.

Moreover, by using "not exclusive to", the language of the document suggests flexibility, which (again) includes online activities that could indicate the user's identity.

Additionally, the protection of personal data is guaranteed in this document by prohibiting the leakage of personal data. This certainly includes the leakage of data for advertising purposes as well. Moreover, if retaining data that could identify users is forbidden under Section 4, selling this data to advertisement companies should receive a stronger punishment for violation. Finally, the language of Section 5 shows the legislature's intention in covering all aspects to protect data privacy.

8.7 Additional Legal Instruments

The Cloud Computing Framework (2019)

The Cloud Computing Framework[1] regulates the relationship between cloud service providers (CSPs), individuals, government bodies, and corporations. Specifically, the law includes principles of data protection requiring registration of content classification with the CITC.

The framework also obligates CSPs to adhere to cloud security requirements. Cloud customer information is categorized into different levels based on the necessary level of protection, which depends on the information's privacy and integrity (sensitive, non-sensitive, government body, private sector, etc.).

Although not directly related to the issue of behavioural targeting, this law articulates the legislature's intent to protect personal data from any form of breach.

Anti-Cyber Crime Law (2007)

Article 2 of the Anti-Cyber Crime Law[2] aims to reduce the occurrence of cybercrimes through:

- Seeking to guarantee the security of information.
- Safeguarding rights concerning the legitimate use of computers and information networks.
- Protecting public interest, ethics, and the national economy.

The law, however, does not elaborate on the issue of cyber data protection. Nonetheless, the law requires an individual's consent to process their data, including disclosing any documents obtained by such processing.

8.8 Personal Data Protection Law (PDPL)(2021)

In September 2021, the long overdue Personal Data Protection Law[3] was issued with the purpose of data protection for individuals and regulation for the collection, processing, disclosure, or retention of personal data through organizations. This long-awaited law is meant to cover shortcomings of other privacy-related provisions and is expected to go into effect in 2023. The Saudi Data and Artificial Intelligence Authority (SDAIA) will be the body overseeing the implementation of the PDPL.

[1] Cloud Computing Framework (2019). https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/CCRF_Ar.pdf
[2] Royal Decree No. M/17 (2017). [online] https://www.mcit.gov.sa/sites/default/files/la_004_a_anti-cyber_crime_law.pdf.
[3] Royal Decree No. M/19 (20121). [online] https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1

The PDPL specifies the conditions that organizations collecting and processing personal data must abide by. Further, PDPL also specifies the rights of data subjects and the penalties for violating the law. A special characteristic of the PDPL is that it does not prevent data subjects from enjoying any greater protection provided by any other related law or regulation.

Article 5 of the PDPL requires organization collecting personal data to obtain the consent of data subjects (except for a few exceptions regulated by the law where a greater public or private interest is at risk if another law or previous agreement to which the data subject is a party requires so, if the data is collected for security or judicial reasons, or if the data is collected for scientific, research or statical reasons).

Organizations are also obligated under the PDPL while collecting personal data to notify data subjects of:

- Data subjects' rights
- The reason for data collection, whether it is optional or mandatory, and to assure data subjects that their data will not be used in any other means.
- Identification of the person collecting data
- Any third-party organizations involved will be able to access the data.
- Potential risks for not completing the data collection process.

Thus, the PDPL offers greater protection to data and ensures its privacy. However, the PDPL has failed to address behavioural targeting or regulate the practice in a way to forbid its existence and protects the privacy of internet users.

8.9 Takeaways of the Legal Analysis

Behavioural targeting is not explicitly illegal. However, the analysed legal instruments create a framework in Saudi Arabia to protect against behavioural targeting through an emphasis on the privacy of personal data. The challenge is the enforcement of the legal framework in a way that prevents behavioural targeting, which is necessary to protect the privacy of internet users. The problem is not the insufficiency of relevant laws. However, information technology-related laws are different from other laws. Traditional laws are usually stable and deal with long-term events and situations. The pace of change is much faster in the technological world; thus, technology-related laws should not progress at the same pace as traditional laws. Technology laws should require constant updates to keep up with ever-changing developments.

Therefore, a law with specific mention and guidelines on behavioural targeting and a law that balances advertisement companies' interests and users' rights to privacy is critical to limit this practice of invading users' privacy.

9. Conclusion and Recommendations

Behavioural targeting is a serious yet neglected issue. ISPs are selling users' data to advertising companies, which can easily identify those users which is a clear invasion of privacy. Unfortunately, the benefits of behavioural targeting to advertising companies appear to override the negative impact on internet users, especially since users themselves often lack awareness of the magnitude of the issue.

The reality is that ISPs obtain approval to collect data through privacy statements; however, due to statements' technical language and length, users are accepting what they do not understand. Hence, clear and informed consent is necessary to ensure the transparency of the process.

As stated, the root of the issue is not exactly the absence of legislation. Even though behavioural targeting is not prohibited directly, many laws and regulations can be used to forbid the practice

as previously analysed. However, behavioural targeting continues due to a lack of user awareness coupled with the substantial economic benefits to the advertisement industry, as well as the sellers of consumer goods and services. The benefits of enforcing relevant laws and the protection of private data carry less weight than the negative impact of reducing advertiser access to individuals.

Accordingly, the following recommendations could protect the privacy of individual users online

- Create an alliance of concerned governmental bodies (SDAIA, the Ministry of Commerce, the Ministry of Communications, the Ministry of Media, and the CITC) that distributes the burden of monitoring, following up, and preventing the practice of behavioural targeting of consumers in Saudi Arabia, while allowing concerned ministries to jointly review the legal framework and prevent legal loopholes.
- Monitor the practice and issuance of clear guidelines and a framework for behavioural targeting by the SDAIA as the concerned body.
- Educate the public about data privacy and the consequences of behavioural targeting.
- Require ISPs to obtain clear and concise consent from users to use their data for advertising purposes instead of hiding this provision in lengthy privacy statements.

10. Sources and references

Books

Esposito, Dino, Programming Microsoft Asp.Net 2.0 Applications, Pearson, Redmond, 2006, 538.

Journal articles

1- Hotaling, A. (2008) ‘Protecting Personally Identifying Information on the Internet: Notice and Consent in the Age of Behavioural Advertising’, *CommLaw Conspectus*, Vol. 16, pp. 529–565, 530.

2- Boerman, S. et al. (2017) ‘Online Behavioural Advertising: A Literature Review and Research Agenda’, *Journal of Advertising*, Vol. 46 No. 3, pp. 363–376, at 367.
3- Hoofnagle, C.J. et al. (2012) ‘Behavioural Advertising: The Offer You Cannot Refuse’, *Harvard Law & Policy Review*, Vol. 6, pp. 273.
4- Sprague, R. and Ciocchetti, C. (2009) ‘Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws’, *Albany Law Journal of Science & Technology*, Vol. 19 No. 1, pp. 91–140.
5- Berger, D. D. (2010) ‘Balancing consumer privacy with Behavioural targeting’, *Santa Clara Computer & High Technology Law Journal*, Vol. 27 No. 1, pp. 3–62.

Laws and regulations

1- Basic Law of Governance (1992). https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/16b97fcb-4833-4f66-8531-a9a700f161b6/1

2- Ministerial Decision No. 53 (2018). https://www.citc.gov.sa/ar/RulesandSystems/Bylaws/Pages/TelecomActBylaw.aspx.

3- Royal Decree No. M/126 (2019). [online] https://mc.gov.sa/ar/ECC/Pages/default.aspx.

4- Reduction of Spam Regulatory Document (2018). https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT010A_Regulation_For_The_Reduction_of_SPAM_Ar.pdf.

5- Royal Decree No. M/18 (2007). https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_003_%20A_E-Transactions%20Act.pdf

6- Data Privacy Principles for ICT (2020). https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/ReductionofSPAM/Documents/IT010A_Regulation_For_The_Reduction_of_SPAM_Ar.pdf.

7- Cloud Computing Framework (2019). https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Documents/CCRF_Ar.pdf

8- Royal Decree No. M/17 (2017). https://www.mcit.gov.sa/sites/default/files/la_004_a_anti-cyber_crime_law.pdf.

9- Royal Decree No. M/19 (20121).

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1

Websites (online)

1- Barbaro, M. and Zeller Jr., T. (2006) 'A Face is Exposed for AOL Searcher No. 4417749', *New York Times* [online] 9 August. https://www.nytimes.com/2006/08/09/technology/09aol.html
2- *Saudi Arabia: Reaching the Consumer*. [online] https://santandertrade.com/en/portal/analyse-markets/saudi-arabia/reaching-the-consumers (Accessed 28 August 2020).
3- *Saudi Arabia Social Media Statistics 2019*. [online] https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/ (29 October 2019).
4- 2018 CIGI-Ipsos Global Survey on Internet Security and Trust. [online] https://www.cigionline.org/internet-survey-2018#:~:text=The%202018%20CIGI-Ipsos%20Global%20Survey%20on%20Internet%20Security,privacy%20and%20the%20power%20of%20social%20media%20platforms (Accessed 31 August 2020).
5- *Saudi Arabia: Reaching the Consumer*. [online] https://santandertrade.com/en/portal/analyse-markets/saudi-arabia/reaching-the-consumers (Accessed 28 August 2020).
6- *Saudi Arabia Social Media Statistics 2019*. [online] https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/ (29 October 2019).
7- *The State of Social Media*. (2020) [online] https://www.crowdanalyzer.com/hubfs/Reports%202020/SOSM%20Report%2020_ENG_Final_May.pdf (Accessed 1 September 2020).
8- Albanesius, C. (2008) 'Should Your ISP be allowed to Serve You Spyware?', *PC Magazine* [online] 28 April. http://www.pcmag.com/print article2/0,1217,a=226952,00.asp?hidPrint-true
9-

Interviews

Interview with Dr. DaifAllah Alzahrani (Deputy Governor for Competition and Legal Affairs at the Commission of Communication). (26 July 2020).