International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13 Issue 3, March, 2024, Impact Factor: 8.285

# Privacy-Preserving Marketing Analytics: Navigating the Future of Cookieless Tracking

Mickey Singh

Marketing Analytics Manager, Affirm Inc. MS in Applied Statistics from Rochester Institute of Technology, NY"

## INTRODUCTION

This paper aims to present a network analysis of online behavioural advertising and tracking, examining scientific studies on data mining and inference techniques applied to individuals, while also addressing the practical implications for both individuals and society as a whole. The goal is to develop a comprehensive model that encompasses the precise technical methods utilized in the industry, as well as the social consequences of these methods. Building upon previous privacy research, we propose a multi-faceted approach to safeguarding consumer privacy in online advertising. This approach involves empowering individuals through the provision of tools and information, fostering the development of privacy-enhancing systems and technologies for advertisers, and implementing industry regulations to enforce fair privacy practices and data protection standards. (Krishen et al.2021)

Numerous digital analytics systems rely on monitoring the online conduct of individuals across various websites. While these systems prove advantageous for websites and marketing groups, they generally do not benefit the individuals being monitored. Typically, the collected data is utilized to influence an individual's purchasing patterns or even predict and manipulate their behavior in other areas, like voting. From the perspective of the tracking entity, influencing behavior may seem harmless, such as displaying more ads related to the individual's interests. However, it can also lead to actions that are not in the best interest of the individual or society. A study revealed that by deducing certain personality traits, political messages can effectively sway the voting preferences of individuals with those traits, even going so far as dissuading them from voting altogether. Digital advertisers may perceive such research as an opportunity to alter the habits of individuals who possess certain characteristics, benefiting them but potentially harming the individuals in question. Furthermore, often individuals are unaware of the tracking that enables such influence, and even if they were aware, understanding or controlling how the inference about them was made can be challenging. Inferring information about individuals is vital for many marketing and analytics practices, and in most cases, the inferences that hold the greatest value for advertisers or data analysts are the ones individuals would least want to be disclosed or acted upon. This power and information imbalance concerning tracked individuals fundamentally raises privacy concerns. This contradicts the scenario where data is collected with an individual's fully informed and voluntary consent, which many privacy definitions exclude from the concept of privacy violation. (Bulotano et al.2023)

### Importance of Privacy-Preserving Marketing Analytics

The goal of marketing analytics is to understand how advertising products, whether they be specific products being advertised or the advertising itself, influence consumer behaviour. Such influence can take on many forms, from memory of the product or brand to changes in consumer purchase decisions. In the field of economics, consumer behaviour analysis is often done through creation of models based on theoretical consumer types or assumptions. These models are then tested through observation of consumer reaction to changes in the economic environment. Advertising and consumer behaviour tracking uses similar methodologies to understand consumer reaction to a specific advertising product and how consumer preferences can be influenced through changes in specific product variables. The data used for such analysis can be of both aggregate and individual form, where aggregation of data might be used more for understanding macro level market trends and brand image, and individual data might be used to understand specific consumer segments and how they are influenced by specific product types. A common way to obtain consumer behaviour data is through the use of surveys, though in the case of advertising impact it is more desirable to obtain data in a way that does not require deliberate consumer effort, as this will ensure that obtained data is a true reflection of consumer behaviour. More indirect data collection methods are often not observable by the consumer and can involve collection of any data that is recorded when a consumer interacts with an advertising product. This might involve changes in consumer online behaviour on a site that the advertising product links to, or changes in online behaviour at sites that sell a product that the consumer has been led to through the advertising product. Data collection can also be done in a way that the advertising product provider observes the data that the consumer

wishes to keep private e.g. changes in behaviour of those seeking advice on a specific medical condition. (Aljumah et al.2021)

In today's highly connected world, marketing initiatives have become a ubiquitous part of life. Consumers are constantly bombarded with products and services being offered to them by advertisers. One might argue that with such a deluge of marketing messages, it is becoming increasingly difficult for consumers to make informed decisions about the products and services being offered. Similarly, small and medium size businesses, who are often faced with the challenge of reaching a large number of potential customers in a cost effective manner, find it difficult to measure the effectiveness of their advertising efforts. These trends have intensified with the growth of the Internet, prompting businesses and researchers to seek new ways of understanding how consumers navigate the information ecosystem and the effectiveness of different advertising strategies on consumer behaviour. (Moustakas et al.2020)This phenomenon has sparked a global, computational arms race between advertising platforms and content providers seeking to provide marketing analytics tools, and technologies to help understand consumer behaviour and advertising impact. Techniques for collecting data about advertising impact and consumer behaviour span both on and off-line settings, and have serious implications on consumer privacy. This paper focuses on the privacy implications of marketing analytics technology and practice, with a specific examination of online advertising and its effects on consumer privacy. Because advertising analytics can be based on the data collected from deployment of the advertising product, this work focuses on a specific instance of advertising technique known as search-targeted-text advertising, in which advertising analytics is done through collection and analysis of private data obtained from consumer search queries.

**Challenges of Cookieless Tracking**

At the heart of cookie use in online tracking is the storing of uniquely identifiable information. This allows for the aggregation of a user's session history, which in turn enables long-term detailed analysis based on their activity. Some cookies have expiry dates, some are session-specific, and their data can either be erased upon completion of their respective site visits or stored indefinitely. Usually, this provides little benefit to the actual website visitor, as data is collected without their awareness. Any privacy-preserving solutions must consider the risk of personally identifiable data matching with data already collected, as it may be stored and forgotten in the sea of third-party data storage. (Thomas, 2021)Additionally, data accuracy is crucial when users can potentially be tracked over a number of years. Finally, any automated methods of data collection should not discriminate against users who choose privacy opting out. Any forced redirection or lesser functionality for non-tracking users would be unacceptable.

The core of privacy marketing analysis comes from cookie tracking for a company's website. A cookie is an identification assigned to a website visitor's computer, providing identification and tracking services. It uses the legacy method of third-party browser cookies for online tracking by default, but does not track or collect any uniquely identifiable information regarding visitors. As regulation has continued to evolve and a broader range of industries are using online marketing analysis, there has been an increasing need to develop solutions that are not only legally compliant but also truly privacy-preserving. (Papadogiannakis et al.2021)(Cooper et al.2023)

**Purpose of the Work**

The goal of this work is to assist marketers and marketing analysts in their task of efficiently targeting consumers with marketing activities that are also privacy preserving. This necessarily involves understanding the new landscape of digital tracking, developing new privacy-preserving tracking methods, and taking steps to maximize the accuracy of these methods. As such, the work will detail new marketing technologies, review legal and computer science literature related to digital tracking and privacy, and delineate new methods for privacy-preserving tracking and assessment of tracking accuracy. The intended outcome for the reader is a thorough understanding of the upcoming changes in digital tracking, the ability to locate and track current and future digital marketing activities in terms of privacy and accuracy, and the knowledge to mitigate privacy risks and maximize tracking accuracy. A secondary purpose of the work is to assist consumer advocates and privacy researchers in understanding marketing tracking technology and its privacy implications, and to provide new methods for consumer advocates to track digital marketing activities aimed at them, assess privacy risk, and create evidence-based arguments for better privacy practices in the marketing industry. (Macha et al.2023)(Koch et al.2020)

## UNDERSTANDING COOKIELESS TRACKING

There are various other issues surrounding the use of cookies, but inevitably the question arises, are they here to stay? Increasingly, internet users are turning to software tools in an effort to block or control cookies. These tools protect user privacy by preventing the covert collection of data regarding their online activities. In light of these developments, cookies may soon become an unreliable source of information about how users interact with websites. Additionally, the credibility

of information from cookies is being compromised by the increasing instances of cookie deletion and the sharing of computers. (Jansen, 2022)(Hils et al.2020) In their zealousness to rid computers of intrusive adware, many users are eradicating all cookies and are unaware of the negative effects this has on their web surfing experience. Given these trends, a replacement for the cookie-based tracking model is required. Understanding the evolution and reasons for the obsolescence of cookies is important in evaluating the necessity and function of cookieless tracking methods. An analysis of alternatives to traditional cookies will provide insight into future technologies that are likely to influence how data is collected and interpreted. Finally, evaluations of benefits and limitations of cookieless tracking relative to its predecessor will gauge whether it is a positive or negative development in the realms of marketing and user experience on the internet. (Geradin et al., 2020)

**Definition of Cookieless Tracking**

By April 2022, all major web browsers have phased out third-party cookies, marking the start of a new world without third-party cookies. It was a movement headed by Safari and Firefox and backed by Google's manifesto clarifying its intent to phase out cookies. Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have implemented significant constraints on cookie usage and third-party data sharing. Ad-technology companies and digital marketers are standing at the edge of a turbulent ocean of change. In the new world, digital media will be anything but business as usual. (Elmér and Nilsson, 2023)

Without cookies, data tracking will be as simple as a ship navigating the open sea. The idea of knowing exactly who, when, where, and how a user has engaged with any aspect of digital media will become unrealistic. While there are some who are celebrating the idea of an ad-tech apocalypse and a complete annihilation of tracking, those who rely on fundamental metrics of digital media behavior are seeking ways to maintain some semblance of simple user tracking. (Bojic, 2022)This is where alternative data tracking methods come into play. A simple definition of tracking can be described as foreseeing, following, and moving along the same path as another object or person. The common progression of understanding user behavior is analogous to an investigator following a trial. The investigator is trying to discern what route the suspect has taken and what decisions the suspect had made. When answering questions related to user behavior, an investigator uses evidence to form a conclusion. If a user's actions are his/her evidence, then the investigator requires some way to discern and catalog that evidence. (Pramanik et al.2021)

**Alternatives to Traditional Cookies**

The promise of cookieless tracking doesn't necessarily mean the end of cookies. They just won't be the primary method of tracking a user's activity. Traditional cookies, as mentioned above, rely on the user to input personal information. There are also third-party cookies, which track a user's activity through multiple sites. A study done by comScore Networks showed that third-party cookies accounted for 66% of all cookies set on computers that were part of their research. The distinction between the two types of cookies is important; many users do not mind first-party cookies because they are taking place on a site that the user intends to visit, and they are often gathering personal login information to improve user experience. (Miller and Skiera, 2023)(Feal et al.2021)Third-party cookies are what make the least of the privacy-sensitive stir up amongst internet users, as they track user activity across sites and sometimes sell the information to other companies. This method of information gathering is what cookieless tracking is trying to avoid, and what legislation is attempting to prevent by limiting the time frame of the cookie's storage, and requiring user consent. As related to cookieless tracking, the alternative placement of a third-party cookie is often an internet tag or pixel placed on a web page, which sends data to another server about that user or the page contents. This method can often take place without the user's knowledge as well, making it a similar target of privacy-related legislation.

**Benefits and Limitations of Cookieless Tracking**

Before delving into a discussion of cookieless tracking, it is necessary to understand the idiosyncrasies of traditional cookies, their benefits and limitations. This understanding will shed light on why marketers and researchers have employed cookies for so long and why they are now seeking cookieless alternatives.

Traditional cookies have many benefits: they are easy to implement, data is easy to collect, and they facilitate the storage of vast amounts of user data for future use. As a result, companies can now collect vast quantities of data on their users' browsing behaviour and store it indefinitely. It is this last feature of persistency which has caused much concern among privacy advocates. Traditional cookies do not expire for months, or even years. If a user knew how much data was being collected about them and had the choice, it is likely they would still permit the storing of only a small fraction of it. (Geradin et al., 2020)

Furthermore, this stored data can be used to construct detailed profiles of users which can then be sold to or exchanged with other companies. The ability to profile essentially has turned the tables on the essence of marketing from a focus on product

placement and promotion, to the targeting and tailoring of products to specific consumer groups. This has made it a much more invasive practice for consumers and has often led to user alienation, on the other hand, benefiting the marketers immensely. (Mehta, 2022)

Through detailed consumer profiles and analysis of browsing behaviour, companies can now evaluate the effectiveness of their online marketing efforts, determine consumer needs and reactions to certain products, and conduct market research all of which more cost-effectively than previous methods.

## PRIVACY CONCERNS IN MARKETING ANALYTICS

The integration, management, and analysis of consumer data concerning privacy concerns as well as digital interactive marketing practices raise tough challenges to accepted and legitimate practice of marketing analytics for many firms. The dangers inside this issue are rising as markets are becoming global and electronic in their nature. Several major reasons for this happening are due to the global reach of the internet as well as the pace of technology development making it easy for consumers to trade their privacy for a small economic incentive i.e. coupon, discounts, etc. The economic value of data is so significant in developed and developing countries that public laws and regulations concerning consumer privacy and protection lag behind the uninhibited flow of information. On account of this, consumers have become increasingly concerned over their personal privacy. (Omar and Inaba, 2020)

As noted by Malhotra, Kim, and Agarwal (2004), in a survey concerning the internet privacy paradox, finds that internet users have a high level of concerns about privacy issues but feel that the benefits of providing personal information outweigh the cost of privacy itself. This mainly occurs in situations where an individual is provided an economic incentive for provision of information. An example would be an online consumer that has just purchased airline tickets visiting a car rental site. (Alwarafy et al.2020)An internet user on a car rental site may be offered cheaper rates on a rental by providing information concerning the airline tickets he has just purchased. The user would see this as beneficial since the information he provides influences in saving more money and benefits him in receiving a cheap car rental price. At the same time, users here fear that the provided second source information on the airline tickets may be connected into an aggregate profiling an individual with intention of discriminating prices of future airline ticket purchases. With the continuous growth of technology coupled with data integration innovations today, the ability to trace activities across internet domains and link them to a specific identifiable individual has created an environment of vast monitoring capabilities. Guidance on these concerns lead marketing analytics into boundaries of what is known as "ethical considerations". (Javaid et al., 2021)(Javaid et al.2021)

### 3.1. Overview of Privacy Issues

There will be times when marketers, especially those who are working in the area of retail, would like to know what individual consumers are doing with respect to the product being considered. A marketer will look at habits of the consumers in terms of whether they are buying the product of interest, how often they are buying the product, and whether or not they are buying the product for continued use. Often it is the case that there are different segments of consumers, and the marketer would like to compare the aforementioned consumption habits on one segment relative to the other. (Alzoubi et al.2022)

Do note that in this paper, our focus is on analytics done using data that is computer processable, rather than a focus on qualitative market research. While market research is very important and can provide useful qualitative information for a marketer, it is beyond the scope of what can be accomplished in a privacy-preserving manner.

The most straightforward way to understand consumer behavior is to just track a consumer's actions pertaining to the product of interest, and then correlate revealed preference with a variety of observed properties about the consumer. In the context of web advertising, consumer on-site actions and observed properties map closely to events on a website and the cookies set by the web-advertiser. This is the interpretation of marketing analytics that is most beneficial for the advertiser, as success is measured by how close the marketing analytics comes relative to what was uncovered. For most cases, the consumer's desired results of advertising are accomplished privately, without any donation of consumer information. Therefore, the task of privacy preservation is to uncover marketing analytics without actually needing to communicate with the consumer or storing any specific information related to the consumer. (Buhalis and Volchek, 2021)

**Legal and Ethical Considerations**

International online privacy legislation is complex and ever-developing. The European Union, comprised of 27 member nations, has taken a lead in privacy regulation with the European Directive that requires data processing of EU citizens' personal information to meet a series of rigorous requirements. The Directive has been legislated differently across the EU jurisdictions, using the EU Commission which makes negotiation heavy and enforcement somewhat patchy. The Data

Protection Act enforces the EU Directive in the UK, making way for the strongest data protection legislation in the world. Several member states including Germany and Spain have opted for different requirements for certain data processing such as even stricter requirements for sensitive personal data. New amendments to the Directive will require that all member states legislate to implement the new laws. This has posed a large challenge to the online advertising industry to change businesses practices or even technology to deal with different requirements within the European nations. Failure to meet these requirements will result in heavy fines and potentially civil actions brought by individuals. This is particularly relevant to transborder data processing such as cloud computing where it may be unclear the jurisdiction in which the data is being processed. Failure to meet legislative requirements may cause third party data processors to be liable rather than the publisher or advertiser whom the requirements were to protect. This can cause uncertainty within business relationships as to who should bear cost of compliance requirements. (de et al.2020)

**Consumer Trust and Transparency**

One of the key issues concerning consumer protection is the consumers' willingness to trust firms with information. Consumers are comfortable with the industry practice of gathering data for marketing purposes, but leery about their data being used in ways other than what was originally intended or shared without their consent. Studies have shown that once it is revealed to consumers how much data mining is actually done, they are shocked and the level of trust they once had for a firm significantly decreases. In order for the online environment to prosper, consumers must be confident that their welfare is not being compromised. (Jones et al.2020)

Transparency is one of the key tactics to ensuring consumer trust. The traditional definition is the quality of something being easily seen through, detected or understood. In the sense of privacy, it means that a company's data management practices and the effects of these practices on consumers are open and obvious to consumers and have been communicated in a manner in which the consumer understands. At first search, this would seem like a convenient measure to increase consumer trust, however, in some cases, it would reveal so much information to the consumer that it would actually damage the consumer's perception of the company in question. With the current level of misunderstanding by consumers of what actually goes on with their data, a sudden full disclosure could have severe repercussions. This method requires a medium in which the most relevant information about data practices can be conveyed to consumers without exposing unnecessary information that may harm the company-consumer relationship. (Guo et al.2022)(Kwan et al.2021)

## TECHNIQUES FOR PRIVACY-PRESERVING MARKETING ANALYTICS

To achieve privacy while analyzing data, the marketing analysts may enable the access of the client, with which he can access the database, but he will have no way to identify the people to which the data corresponds to. This is known as third-party certification. However, this approach proves to be ineffective in the day and age with powerful statistical packages or even data mining techniques, as it would not be too hard to get the original data and compare the results to identify people. To counter this, global generalization can be carried out before the query results are released to the client. Generalization involves replacing a data value with a less specific but semantically consistent value. This is done so that it will be impossible to map the results back to the original data, therefore ensuring identity privacy is kept. (Wieringa et al.2021) This can be done by simply categorizing all attribute values into different sets and then replacing the data with values from a less detailed set. For example, someone's age can be categorized into young (0-17), adult (18-65), and old (65+), and then the actual age figure will be replaced by anyone in that range. This type of generalization would be termed K-anonymity, as you need a set of at least K-1 respondents who have the same generalized data. Although this method is effective for identity privacy, it may not prove very effective for answering the client's queries, as much of the data would be too vague and lack the required detail. L diversity is an enhancement of K-anonymity which achieves a better trade-off between privacy and data usability. The basic idea is to protect against attribute disclosure by ensuring that each of the K equivalence classes has at least L well-represented values of some sensitive attribute. This ensures privacy not only in terms of identity but also in terms of the diversity of the data. (Mahanan et al.2020) Privacy-preserving data mining, a relatively new scheme, combines the advantages of general data anonymizing and still being able to apply many more useful data mining algorithms to the modified data to protect and enhance data's utility and mining potential. This is the method we aim to do our AHP assessment on, to compare it both in terms of maintaining privacy and retaining effectiveness. A much stronger form of generalization is that of suppression. This involves not only replacing attribute values but sometimes the removal of whole tuples or rows of data which contain specific values. Though this is an effective method of maintaining privacy, it greatly reduces the amount of data provided and therefore reduces the detail that can be attained from the results. The last method is that of top or bottom coding, which involves replacing extreme attribute values with less specific but still consistent values. This is done by defining a range of acceptable attribute values restricting what can be classed as sensitive and therefore private data.

**Anonymization Methods**

Depending on the nature, some customer data is sensitive and might not be capable of being shared with marketers. In these situations, it becomes necessary to produce anonymized data which would replace this sensitive data with common data but safeguard the identities of the info-rippers. This allows marketers to evaluate the entire dataset and formulate personalized offerings that will be relevant to certain groups, while still protecting the privacy of individuals in the whole dataset. Anonymization generalizes data by stripping intent from it, limiting the quantity of inferences that can be made from it, and removing linkages among different data sets. Anonymized data, in general, has negligible loss of data utility and as a result provides a good trade-off between privacy and utility. This is in contrast to deletion and suppression of sensitive data, which produce a better trade-off between privacy and data utility but may not give marketers enough data to evaluate or formulate precise offerings. Deletion and suppression also only safeguard data in specific databases or systems and don't deal with the problem of preventing leakage of sensitive data from these systems, which might also intertwine with lack of control of how the deleted data will affect downstream systems. (Peethambaran et al.2020)

**Differential Privacy**

Differential privacy is a recently introduced privacy concept that seeks to maximize the accuracy of queries from statistical databases while minimizing the chances of identifying its data subjects. Queries generally consist of a set of conditions to be determined, a function to be applied to the specified data, and an output consisting of the result of that function. A query is said to satisfy differential privacy if the probability of it returning the same result with the inclusion or exclusion of a single data subject from the database is approximately the same. More simply, it is a property of the process of a query on a database. A stronger form of differential privacy considers the case where after executing the algorithm under consideration, the output is to be given to an adversary who, via some auxiliary information about the data subjects involved, aims to determine whether a specific individual participated in the database which the algorithm queried on. The goal here is to maximize the probability of errors in the inference of participation of a specific data subject. Differential privacy offers a highly general means to analyze algorithms in terms of the privacy loss from their executions. It is suited to marketing analytics in that a broad range of queries can be made on statistics gathered from users of the target product with the goal of ascertaining what correlations hold between their behaviors and how this will affect the marketing strategy. (Ghazi et al.2021) Each such query may be tested to see how it might best predict some form of user behavior and could be seen as a separate algorithm in the attempt to find this out. By assigning a privacy budget to a campaign of such queries, one can control how much privacy is lost in trying to determine how best to predict user behaviors from the gathered data. Since such algorithms are usually subject to modifications based on their error rates, it may be possible to use specific forms of query in machine learning with differential privacy constraints as a direct means of optimizing the tradeoff between knowledge gained about the data and privacy lost. (Colnago et al.2020)

**Federated Learning**

Federated learning is a machine learning setting where many clients (here it could be different companies doing digital marketing) train a model under the orchestration of a central server (here it could be a server provided by a marketing analytics company). Each client's raw data samples do not leave the client's device, and model updates are the only things being collected. We can use federated learning to build a global marketing attribution model without sharing data. The company (consumer) trains a local model (on its marketing data), and only the model parameters are included in the updates and transmitted to the central server. This approach is a generalization of the classic "learn and combine" strategy. This "each one teach one" data strategy allows complete control of sensitive data. It can stay on the client's device, halt the learning at any time, and is safe in the knowledge that only a summary of their model will be sent to the server with no chance of the data being used by a third party. (Aledhari et al., 2020)

**Homomorphic Encryption**

Homomorphic encryption is a special form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The homomorphic property is a desirable security feature when outsourcing the storage and computation of data to commercial and public clouds. Consider an organization which has amassed a large dataset of sensitive information. The organization wants to allow a third party to perform computation on the data, but does not want to reveal the data to the third party. With homomorphic encryption, the organization can encrypt the data and allow the third party to store the data and perform computation, without ever revealing the decrypted information. (Lauter et al., 2022)The result of the computation is also encrypted and can be securely sent back to the organization to be decrypted and viewed. If the encryption scheme is at least somewhat homomorphic, this entire process can be carried out without revealing any sensitive information to the third party. In the context of privacy preserving marketing analytics, homomorphic encryption can be applied in the same way. A company that has customer data and a model for marketing analytics could send the encrypted data to a third party which offers computation services for running the model on the data. The third party could perform the computation specified by the model with the encrypted data and return only the encrypted result to the company. Assuming the encryption scheme

used to encrypt the data is the same as the encryption scheme used to encrypt the result, no sensitive information is ever revealed to the third party and the result of the computation can be securely decrypted and viewed by the company. (Alharbi et al.2020)

## EVALUATING THE EFFECTIVENESS OF PRIVACY-PRESERVING TECHNIQUES

Once we understand which of the various privacy risks are critical for users, we would like to accurately assess the extent to which different systems and approaches succeed in mitigating these risks. From a broad perspective, we are looking for quantitative measures of the loss in utility (in the context of marketing and analytics) due to privacy preservation, and the impact of different systems on the accuracy of data analysis. We believe that it is essential to understand which types of analysis are being used in practice, and the precise mechanisms by which they derive value from data. While it is well understood that the primary use of cookies in marketing and analytics is to track user behavior over time, very little is understood about the precise types of analysis which are being used, and which forms of derived data are the most valuable to marketers. To this end, we hope to analyze the effectiveness of our privacy-preserving techniques with respect to specific kinds of analysis and derived data. (Gupta et al.2020)

It is important to distinguish between various privacy risks at this stage, as different methods of data analysis and derived data have differing privacy implications. For example, the loss of information due to the inaccuracy of specific ad targeting may be of less concern to users than the release of personally identifiable information about them, or the existence of a profile that has been built up about them over time. By understanding how different forms of data analysis derive value from data, and the privacy implications of each form, we can tailor our privacy-preserving techniques to specific analyses in order to maximize the utility of derived data relative to privacy risk. This may involve allowing certain types of analysis to be conducted on certain forms of restricted data or implementing global restrictions on certain types of analysis in order to prevent the creation of high privacy risk derived data. (Saura et al.2021)

### Metrics for Assessing Privacy Preservation

In order to effectively evaluate different privacy-preserving techniques, quantitative metrics are needed. Focusing on the process of collecting and analyzing user-specific data for marketing and personalization, Acquisti et al. outline three essential types of data source that can be used for generating metrics for privacy preservation. From this, we consider content data, data about data, and contextual data. Content data refers to the actual user-specific data that an organization is trying to protect (e.g., a user's health condition). Data about data is the data that states when, how and by what means content data is stored and its rules of dissemination. Contextual data is an element of data protection that has been largely overlooked in literature; it refers to the wider environment in which the processing of personal data takes place. This can be regulatory, social, economical, temporal or spatial and in some cases privacy breaches may occur not because specific personal information has been compromised, but because there has been a violation to the environment in which the personal information exists. By defining these three data types, we can use them to define an information loss function, which measures the loss in utility between original and modified data. Lastly, we can compare any privacy-preserving technique to a given privacy policy which states the acceptable conditions under which personal data can be processed and/or divulged. By doing this, we can align a privacy-preserving technique with the desired level of privacy protection. (Bleier, 2021)

### Accuracy and Utility Trade-offs

Privacy-preserving related activities tend to reduce the accuracy of the data processes. For a given privacy level, accurate results may be impossible to attain. Some privacy criteria may be obtained only at the cost of major accuracy loss. However, it is important to explicitly quantify the loss in accuracy, to ensure that the data user is in a position to make an informed decision regarding the value of the resulting data. If the cost in accuracy is too high, the data user may decide not to use the data at all. A utility threshold that the results must meet can be determined, below which the data user will not consider the data to be of any value. (Jung2020)

The trade-off between privacy and accuracy is often a complex one. As an example, consider the addition of noise to a dataset to provide k-anonymity. The amount of noise required is dependent upon the specific algorithm and also upon the data itself, particularly the amount of redundancy within the data. An initial study applying noise to medical records data produced some alarming results. The data was obtained from a record linkage system used to search for matches within the Australian population, to prevent multiple treatments being administered to the same patient. Retrieving different treatment records for the same individual is very undesirable. However, in applying noise to this data and examining the effects, it was found that the probability of finding a match dropped significantly, and in some cases fell to zero. The cost in patient safety would have been substantial. This result led to examination of methods to achieve the same level of anonymity with less effect on the utility of the data. (Hernandez et al., 2022)(Yale et al., 2020)

## IMPLEMENTING PRIVACY-PRESERVING MARKETING ANALYTICS

The proposed methods for implementing privacy-preserving marketing analytics carry a common thread. Each technique aims to extract the maximum possible utility out of available customer-level information under the constraints of a browser-based server intermediated information exchange. The utility comes in the form of improved marketing analytics. Our goal is to increase marketing analytics quality by enabling analysis of end user behavior, without necessarily identifying specific individuals. This is reflected by the goals of each technique: derive aggregate statistics about pages viewed and ads seen (without targeting specific individuals), enable analysis of ad-effectiveness, and enable analysis of site usage patterns. These methods have been or are in the process of being deployed to current systems, and in all cases they share a fundamental characteristic: the storage and manipulation of customer-level information outside of the cookie-based or server log-based system. This is an optimistic sign, as it would be relatively simple for marketing and analytics companies to abandon techniques involving personal information if it were not for the fact that the GDPR and other legislation is providing customer-level data ownership with increased protections and rights. This makes the separation of customer-level info and its protections from current methods a promising path to balance customer privacy rights and marketing analytics utility. (Pramanik et al.2021)(Peethambaran et al.2020)

### Technical Considerations and Requirements

By now it is clear that in the cookieless future, marketing analytics systems will still need to persist to support and meet the needs and goals of all their stakeholders with respect to providing actionable and insightful data. To continue to be effective and relevant, these systems must incorporate and embody the new concerns and requirements of the people and businesses that will use them.(Singh M., 2023)

The technical requirements section of this document has already presented and discussed the data control and data protection needs from several different angles. These are obviously very important considerations. But a system cannot effectively operate within these constraints without first understanding what is actually entailed by the new legislation and how it might affect the system in various ways. (Naeem et al.2022)

Therefore, we will now identify and discuss the technical implications of the data protection legislation on marketing analytics systems. This is not just an academic exercise. Requirements need to be effectively translated into working systems. This will be difficult and complex, and the more that can be shared about what is being required and expected, the more likely it is that suitable solutions will be found.

This section will help to provide a clear understanding between those with the legal knowledge and those with the technical knowledge of what needs to be done and how it might be achieved.

### Data Collection and Processing Strategies

Data collection and processing strategies depend on the system architecture and the party responsible for data collection. In a centralized data collection architecture, where data is collected and stored on a single server, that party is typically the website owner. This party might include a third-party data collection company, in which case the data is collected at the behest of the website owner and stored on a remote server. In a distributed system architecture, the data might be collected by a third party at the instructions of the website owner and combined with data from many other sources, stored, and processed in various ways. (Zhong et al., 2022)

For centralized data collection, since the data is collected and stored on the website owner's server, the implementation of cookieless tracking is relatively straightforward. The website owner simply must ensure that no third-party cookies are set during the data collection process, and that data stored on the first-party server does not contain any information that could be used to track an individual user's activity across sessions and/or on other websites. This can be accomplished using the same techniques to prevent unwanted setting of third-party cookies to be discussed in the following section on cookie blocking, and applying them to the relevant data collection points on the website in collaboration with IT and/or web development personnel. (Ullah et al.2023)

### Compliance with Data Protection Regulations

Data privacy legislation and enforcement is increasing globally, and data protection authorities are focusing more on the analytics space. For instance, the public and private sector efforts around online consumer privacy have resulted in self-regulatory programs and enforcement activities globally, such as the revision of the ePrivacy Directive or the proposal and withdrawal of the ISP Data Services Regulation in the US. (Bennett and Raab, 2020)

Now, with the GDPR having come into effect in October 2017 (though not yet to be enforced for two years), the EU has raised the bar for what is considered acceptable in consumer data collection, processing, and storage. It carries provisions that require organizations to maintain data processing records, perform impact assessments on their processing activities, hire data protection officers, and in some cases, require data controllers and processors to obtain prior authorization from data protection authorities. It also places more liability on data controllers and processors – with potential fines of up to 4% of the global annual turnover. (Georgiadis and Poels, 2022)

While there are many highly detailed considerations for web analytics to be compliant with the GDPR, the one that is perhaps most impactful on the current ecosystem is the requirement to obtain prior consent from the user for data processing and storage. This will negate the current default of many tracking activities, which store data unless the user specifies to opt-out. Instead, it will require that users can opt-in to tracking activities, and such consent must be freely given, specific, informed, and unambiguous. This means offerings such as premium services for users who allow tracking will no longer be a valid form of consent. (Breen et al.2020)(Caruccio et al., 2020)

## FUTURE TRENDS AND INNOVATIONS IN COOKIELESS TRACKING

Web analytics has long depended on the stateless HTTP protocol, the use of client-side cookies as a unique user identifier, and the assumption that tracking user activity at the granular level is acceptable. The rise of data protection regulations, such as the European Data Protection Directive, its revision (which includes a "Cookie Directive"), and the General Data Protection Regulation (GDPR), changes that. Moving forward, compliance and privacy architectures are going to impede the use of cookies for tracking and/or require that users be given control over the degree to which they are tracked and their data collected. (Matte et al.2020)Moreover, analytics systems that trade or process data across jurisdictional boundaries, where contradiction between laws can put a company in legal jeopardy, will have to provide assurance that they can comply with a variety of conflicting privacy constraints including purpose limitation, user consent, and data residency. Regulatory obligations are listed before analytics system capabilities because the former will be the primary driver for changes in the latter. (Pramanik et al.2021)Web analytics adopt a mix of privacy-respecting architectures will emerge to address the global matrix of constraints.

This will include "opt-in" architectures where users consent to anonymous, aggregate collection of their data, using first-party contexts that limit data access to that which is necessary for the user's current session and thereby exempt from many regulations, and privacy-preserving methods to collect and analyze user behavior without personalized data collection. (Beg et al.2021)According to a recent survey, 64% of marketers expected the reduction of availability of third-party data would result in increased use of first-party data and collaboration. (Neumann et al.2023)Given the increasing emphasis on privacy and data protection, it is clear that the landscape of web analytics is going through a transformative period. Companies and marketers will need to adapt to these changes by adopting privacy-conscious approaches that respect user consent and prioritize data security. The shift towards first-party data and collaboration highlights the need for organizations to build direct relationships with their users, gaining their trust through transparent and ethical data practices. Furthermore, as the use of cookies becomes more restricted, analytics systems will need to explore alternative methods of tracking and analysis. Solutions that leverage first-party contexts and limit data access to specific sessions can provide valuable insights without compromising privacy. By focusing on anonymous, aggregate data collection, organizations can gain a comprehensive understanding of user behavior while respecting regulatory requirements. Emerging privacy-preserving methods will also play a crucial role in the evolution of web analytics. These methods allow for the collection and analysis of user behavior without relying on personalized data. By anonymizing and aggregating data, organizations can generate meaningful insights while maintaining the privacy and anonymity of their users. (Kreso et al.2021)In summary, the evolving landscape of data protection regulations and privacy concerns is reshaping the field of web analytics. Organizations must adapt to these changes by adopting privacy-respecting architectures, building direct relationships with users, and embracing alternative methods of tracking and analysis. By prioritizing user consent, data security, and ethical practices, companies can navigate the complex regulatory environment while still harnessing valuable insights from their analytics systems.

## CONCLUSION

In our study, we embark on a data-driven approach to forecast product sales for big box retailers. Our study selected the home appliance goods subcategory from a leading retailer. A key scope of the study is to understand what drives sales in this category and provide insights for retailers and manufacturers. With this understanding, more robust procedures can be put in place to forecast sales. Sales can be influenced by many inside and outside variables, some that can be controlled and others that cannot. For the purpose of this study, we will only focus on variables that can be controlled by the retailer or manufacturer. Understanding the seasonality impact on sales is crucial for forecasting. The home appliances goods subcategory is particularly vulnerable to seasonal changes due to the nature of some products. During the summer season,

fans and air coolers will have higher demand relative to the winter season. A calendar-based time series analysis of past sales data was done to understand the seasonal impact on sales. This approach decomposed the time series into trend, seasonal, and residual components. An ARIMA model was installed using the seasonal data for the purpose of forecasting. The model showed to be highly effective in predicting seasonality trends. (Dimri et al., 2020)

**Summary of Key Findings**

Summary of key findings can be easily delivered by showcasing the key findings of the above discussion chapters about archetypes of marketing organizations. From the detailed analysis of each marketing firm and the recommended stages to flourish or convert to the best practice stage, and the threat of falling back to the bad practice stage. This usually points directly to each marketing organization depending on the motives and methods of customer acquisition. There is no best method for the development of each type of organization as every method has its own consequences to every unique marketing firm, and each firm wants to make a decision of highest profitability with minimal consequences/losses.

There are many pros and cons to the development of the transition between bad and best practice and aligning sequence to each, but MindTrust recommends its services based on the analysis provided as the consequences are predetermined and the goal is efficient customer acquisition, taking into consideration that the data drift effects may set organizations back a stage if a violation of customer privacy occurs. Data migration towards advertising platforms focusing on method control and more accountability will increase as the direct correlation to increasing use of data for advertising methods is an expression of the data itself, and it is easier to manipulate and quantify results of data-driven advertising. This is a positive for advertising platforms and advertisers alike, as higher debug-able accountability has been proven to benefit those with empirical evidence of advertising effects. New laws and regulations are a slow but positive change, as seen often with technology outpacing legal matters and no considerations to the consequences and long-term effects. This will prevent further data drift and consequences to customer privacy. MindTrust and the cookieless tracking marketing firms would like to see improvement to move from the 3rd party data stagnation state without violating customer privacy and leaving best practice methods. It is agreed that the band-aid method to skip to using the classic method of customer acquisition will have fewer consequences and regression, but further analysis has shown it is not probable to attain the same data as a 3rd party data method without going through a change of customer data collection.

**Recommendations for Organizations**

Organizations should monitor further for developments on third-party tracking and new techniques in privacy-preserving marketing analytics and assess their own performance in these areas. With the expected decrease in effectiveness of third-party cookies, it would be beneficial for organizations to increase their first-party data collection capabilities. This will involve testing different value exchange scenarios for data collection with consumers to understand their preferences and the nature of consent. Where possible, organizations should look to build direct relationships with their consumers and develop methods to learn from consumer data while providing them with direct benefits. This will serve companies well in any future environment with increased consumer interaction and transition to direct marketing activities. All of the advised actions and research in the recommendations above should be conducted in accordance with the evolving legal requirements and ethical considerations in the area of consumer privacy data protection.

Dependent upon the scale and resources of the organization, different strategies for privacy-friendly marketing analytics may be appropriate with migration through different short and long-term stages. Small to medium organizations may benefit from immediately ceasing involvement in third-party cookies and tracking, tightly controlling data collection and processing, and seeking expert consultation from advisors with clear intentions to monitor developments and act on the second part of these recommendations. Large organizations with heavy reliance on third-party activity may be in a similar scenario to the current NAI opt-out page and find that initial attempts of privacy-preserving analytics with current methods are only feasible interim measures to maintain some form of consumer-insight activity. In these cases, it may be more realistic to move towards maintaining the prevailing consumer-insight methods while diversifying into development or sponsorship of alternative advertising and analytics platforms to track and understand the effects of cookieless third-party activity from the prospects of the publishers.

## REFERENCES

[1]. Krishen, Anjala S., et al. "A broad overview of interactive digital marketing: A bibliometric network analysis." Journal of Business Research 131 (2021): 183-195. swan.ac.uk

[2]. Bulotano, Triah, et al. "Celebrities' Influence on the Students' Voting Preferences." Journal of Humanities and Social Sciences Studies 5.10 (2023): 68-81. al-kindipublisher.com

[3]. Aljumah, Ahmad Ibrahim, Mohammed T. Nuseir, and Md Mahmudul Alam. "Traditional marketing analytics, big data analytics and big data system quality and the success of new product development." Business Process Management Journal 27.4 (2021): 1108-1125. hal.science

[4]. Moustakas, Evangelos, et al. "Blurring lines between fiction and reality: Perspectives of experts on marketing effectiveness of virtual influencers." 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2020. researchgate.net

[5]. Thomas, I. "Planning for a cookie-less future: How browser and mobile privacy changes will impact marketing, targeting and analytics." Applied marketing analytics, 2021. HTML

[6]. Papadogiannakis, Emmanouil, et al. "User tracking in the post-cookie era: How websites bypass gdpr consent to track users." Proceedings of the web conference 2021. 2021. arxiv.org

[7]. Cooper, Dylan A., et al. "Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising." Journal of Consumer Marketing 40.2 (2023): 235-247. chapman.edu

[8]. Macha, Meghanath, et al. "Personalized privacy preservation in consumer mobile trajectories." Information Systems Research (2023). cmu.edu

[9]. Koch, Karl, et al. "Privacy-preserving analytics for data markets using MPC." IFIP International Summer School on Privacy and Identity Management. Cham: Springer International Publishing, 2020. 226-246. arxiv.org

[10]. Jansen, B. J. "Understanding user-web interactions via web analytics." 2022. HTML

[11]. Hils, Maximilian, Daniel W. Woods, and Rainer Böhme. "Measuring the emergence of consent management on the web." Proceedings of the ACM Internet Measurement Conference. 2020. hi.ls

[12]. Geradin, D., Katsifis, D., and Karanikioti, T. "Google as a de facto privacy regulator: Analyzing Chrome's removal of third-party cookies from an antitrust perspective." 2020. archive.org

[13]. Elmér, J. and Nilsson, J. "A FUTURE WITHOUT THIRD-PARTY COOKIES A study of how Swedish small and medium-sized marketing agencies are affected by the loss of third-party cookies …." 2023. gu.se

[14]. Bojic, L. "Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality?." European Journal of Futures Research, 2022. springer.com

[15]. Pramanik, M. Ileas, et al. "Privacy preserving big data analytics: A critical analysis of state-of-the-art." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 11.1 (2021): e1387. HTML

[16]. Miller, K. M. and Skiera, B. "Economic consequences of online tracking restrictions: evidence from cookies." International journal of research in marketing, 2023. sciencedirect.com

[17]. Feal, Álvaro, et al. "Don't accept candy from strangers: An analysis of third-party mobile sdks." Data Protection and Privacy: Data Protection and Artificial Intelligence 13 (2021): 1. imdea.org

[18]. Mehta, P. "Work alienation as a mediator between work from home-related isolation, loss of task identity and job insecurity amid the COVID-19 pandemic." International Journal of Workplace Health Management, 2022. archive.org

[19]. Omar, M. A. and Inaba, K. "Does financial inclusion reduce poverty and income inequality in developing countries? A panel data analysis." Journal of economic structures, 2020. springer.com

[20]. Alwarafy, Abdulmalik, et al. "A survey on security and privacy issues in edge-computing-assisted internet of things." IEEE Internet of Things Journal 8.6 (2020): 4004-4022. arxiv.org

[21]. Javaid, M., Haleem, A., Singh, R. P., Rab, S., and Suman, R. "Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT)." Sensors International, 2021. sciencedirect.com

[22]. Javaid, Mohd, et al. "Blockchain technology applications for Industry 4.0: A literature-based review." Blockchain: Research and Applications 2.4 (2021): 100027. sciencedirect.com

[23]. Alzoubi, Haitham, et al. "Does BLE technology contribute towards improving marketing strategies, customers' satisfaction and loyalty? The role of open innovation." International Journal of Data and Network Science 6.2 (2022): 449-460. growingscience.com

[24]. Buhalis, D. and Volchek, K. "Bridging marketing theory and big data analytics: The taxonomy of marketing attribution." International Journal of Information Management, 2021. bournemouth.ac.uk

[25]. de Carvalho, Renata M., et al. "Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects." SN Computer Science 1 (2020): 1-16. springer.com

[26]. Jones, Kyle ML, Alan Rubel, and Ellen LeClere. "A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics." Journal of the Association for Information Science and Technology 71.10 (2020): 1227-1241. iupui.edu

[27]. Guo, Yuanyuan, Xin Wang, and Chaoyou Wang. "Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern." Journal of Enterprise Information Management 35.3 (2022): 774-795. HTML

[28]. Kwan, David, Luiz Marcio Cysneiros, and Julio Cesar Sampaio do Prado Leite. "Towards achieving trust through transparency and ethics." 2021 IEEE 29th International Requirements Engineering Conference (RE). IEEE, 2021. HTML

[29]. Wieringa, Jaap, et al. "Data analytics in a privacy-concerned world." Journal of Business Research 122 (2021): 915-925. sciencedirect.com

[30]. Mahanan, Waranya, W. Art Chaovalitwongse, and Juggapong Natwichai. "Data anonymization: a novel optimal k-anonymity algorithm for identical generalization hierarchy data in IoT." Service Oriented Computing and Applications 14 (2020): 89-100. HTML

[31]. Peethambaran, Geetha, Chandrakant Naikodi, and L. Suresh. "An ensemble learning approach for privacy–quality–efficiency trade-off in data analytics." 2020 International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2020. HTML

[32]. Ghazi, Badih, et al. "Deep learning with label differential privacy." Advances in neural information processing systems 34 (2021): 27131-27145. neurips.cc

[33]. Colnago, Jessica, et al. "Informing the design of a personalized privacy assistant for the internet of things." Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020. acm.org

[34]. Aledhari, M., Razzak, R., Parizi, R. M., and Saeed, F. "Federated learning: A survey on enabling technologies, protocols, and applications." IEEE Access, 2020. ieee.org

[35]. Lauter, K. E., Dai, W., and Laine, K. "Protecting privacy through homomorphic encryption." 2022. uniwa.gr

[36]. Alharbi, Ayman, Haneen Zamzami, and Eman Samkri. "Survey on homomorphic encryption and address of new trend." International Journal of Advanced Computer Science and Applications 11.7 (2020). semanticscholar.org

[37]. Gupta, Shaphali, et al. "Digital analytics: Modeling for insights and new methods." Journal of Interactive Marketing 51.1 (2020): 26-43. rug.nl

[38]. Saura, Jose Ramon, Domingo Ribeiro-Soriano, and Daniel Palacios-Marqués. "From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets." International Journal of Information Management 60 (2021): 102331. sciencedirect.com

[39]. Bleier, A. "On the viability of contextual advertising as a privacy-preserving alternative to behavioral advertising on the web." Available at SSRN 3980001, 2021. researchgate.net

[40]. Jung, Im Y. "A review of privacy-preserving human and human activity recognition." International Journal on Smart Sensing and Intelligent Systems 13.1 (2020): 1-13. sciendo.com

[41]. Hernandez, M., Epelde, G., Alberdi, A., Cilla, R., and Rankin, D. "Synthetic data generation for tabular health records: A systematic review." Neurocomputing, 2022. HTML

[42]. Yale, A., Dash, S., Dutta, R., Guyon, I., Pavao, A., and Bennett, K. P. "Generation and evaluation of privacy preserving synthetic health data." Neurocomputing, 2020. hal.science

[43]. Naeem, Muhammad, et al. "Trends and future perspective challenges in big data." Advances in Intelligent Data Analysis and Applications: Proceeding of the Sixth Euro-China Conference on Intelligent Data Analysis and Applications, 15–18 October 2019, Arad, Romania. Springer Singapore, 2022. HTML

[44]. Zhong, B., Guo, J., Zhang, L., Wu, H., Li, H., and Wang, Y. "A blockchain-based framework for on-site construction environmental monitoring: Proof of concept." Building and Environment, 2022. HTML

[45]. Ullah, Imdad, Roksana Boreli, and Salil S. Kanhere. "Privacy in targeted advertising on mobile devices: a survey." International Journal of Information Security 22.3 (2023): 647-678. springer.com

[46]. Bennett, C. J. and Raab, C. D. "Revisiting the governance of privacy: Contemporary policy instruments in global perspective." Regulation & Governance, 2020. HTML

[47]. Georgiadis, G. and Poels, G. "Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic …." Computer Law & Security Review, 2022. HTML

[48]. Breen, Stephen, Karim Ouazzane, and Preeti Patel. "GDPR: Is your consent valid?." Business Information Review 37.1 (2020): 19-24. sagepub.com

[49]. Caruccio, L., Desiato, D., Polese, G., and Tortora, G. "GDPR compliant information confidentiality preservation in big data processing." IEEE Access, 2020. ieee.org

[50]. Singh, M. "Unleashing the Power of Big Data Analytics: Examining Its Effect on Marketing Efficiency and Effectiveness in the Digital Era." International Journal of Innovative Science and Research Technology (IJISRT), 8(6), 2023/6[PDF] from researchgate.net

[51]. Matte, Célestin, Nataliia Bielova, and Cristiana Santos. "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework." 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020. arxiv.org

[52]. Beg, Saira, et al. "A privacy-preserving protocol for continuous and dynamic data collection in IoT enabled mobile app recommendation system (MARS)." Journal of Network and Computer Applications 174 (2021): 102874. academia.edu

[53]. Neumann, Nico, et al. "Is first-or third-party audience data more effective for reaching the 'right'customers? The case of IT decision-makers." Quantitative Marketing and Economics 21.4 (2023): 519-571. springer.com

[54]. Kreso, Inda, Amra Kapo, and Lejla Turulja. "Data mining privacy preserving: Research agenda." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 11.1 (2021): e1392. rights-platform.com

[55]. Dimri, T., Ahmad, S., and Sharif, M. "Time series analysis of climate variables using seasonal ARIMA approach." Journal of Earth System Science, 2020. ias.ac.in