The need to focus more on the ethics of the use of personal data in advertising

Paula Mandingorra Sánchez

Computer Ethics, Politecnico di Milano, Italy

Abstract

The use of personal data has become increasingly common to personalize advertising. However, this raises serious questions about privacy and the rights of individuals. The paper discusses the need to focus on the ethics of the use of personal data in advertising. The different approaches used to address the issue are analysed and ethical solutions are proposed. The pros and cons of ethical and unethical uses of information are discussed. In addition, recommendations are offered on how to address the ethical use of personal data in advertising, including the adoption of security mechanisms, the adoption of standards for data use, and the development of a culture of accountability in data use. Finally, an agenda for the future is proposed, addressing the need for greater commitment to ethics and accountability in the use of personal data in advertising.

1. Introduction

The ethics of using personal data in advertising has become an increasingly important issue in an increasingly digitized and connected world. Technology allows us to share and store information more quickly and easily than ever before, creating new opportunities for advertisers to personalize their advertising messages. This personalization is achieved through the use of personal data, and while this gives advertisers a greater ability to influence consumers, it also opens the door to potential abuse.

The use of personal data, however, is not a new resource. From print advertising to online ads, advertisers have collected information about consumers to improve their advertising campaigns. But as technology advances, data collection is becoming steadily more sophisticated. Many companies use user information to create targeted ads, adjusting their content based on what is known about users. This allows advertisers to deliver even more relevant and effective content to their audiences.

However, the use of personal data also raises some ethical and legal issues. There are privacy and human rights concerns, and some people have concerns about the misuse of their data. These concerns have intensified with the emergence of artificial intelligence, which can process enormous amounts of data to predict user behaviour. This can have a direct effect on targeted advertising, raising questions about the responsibility and morality of advertisers.

Because of these concerns, the ethics of using personal data in advertising should be a more pressing topic of discussion. The discussion should focus on how advertisers can ensure the security and privacy of users, as well as the ethical and legal boundaries that advertisers should follow when using personal data. This paper will focus on these issues and seek to establish a framework for the ethical use of personal data in advertising.

2. Algorithms in digital advertising

The digital advertising algorithm is a set of rules and procedures that advertising platforms use to determine how and to whom show online ads. They are based on data about user behaviour, interests and preferences, and use this information to select and deliver relevant ads to a specific audience.

These algorithms have become an increasingly useful tool for companies looking to enhance the efficiency of their marketing campaigns. In digital advertising they are used to maximize the effectiveness of ads, targeting their advertising to the right consumers and saving time and resources.

There are several factors that come into play in ad targeting, including the context of the web page, the user's browsing history and the content of the ad. For instance, if a user visits an e-commerce site, the advertising algorithm can use this information to display ads related to similar products that the user has previously searched for or purchased.

Advertising algorithms also use user demographic and profile information to select ads. For example, if a user is of legal age and lives in a large city, the algorithm may select ads for products or services that are relevant to that demographic.

In addition, advertising algorithms use machine learning techniques with the aim of continually improving their ability to select and deliver relevant ads. They can learn from user behaviour patterns and adapt to improve advertising effectiveness as user preferences and market trends change.

They additionally provide performance optimization techniques to maximize ad performance. This includes A/B testing, where different versions of an ad are compared to determine which is most effective, and adjusting ads in real time to adapt to changes in user patterns and market trends.

The algorithm likewise takes into account the context in which the ad is being displayed, such as the keyword used in a search or the content of the page on which the ad is being displayed. The ultimate goal is to show the user the ads that are most relevant and valuable to him or her.

On the other hand, in the selection and delivery of ads one of the most used techniques is pay per click (PPC), which is used in Social Ads such as Facebook Ads, in which advertisers pay each time a user clicks on one of their ads. This allows advertisers to pay only for the actual traffic they receive through their ads, although pay per impression (CPM) is also used on other platforms such as Google Ads. Therefore, personalized advertising is very important today.

Nonetheless, these algorithms can also give rise to privacy and security issues, as they can collect and use users' personal information without their knowledge or consent.

One common problem is navigation tracking, in which algorithms collect information about the web pages users visit and the products they search for. This information is used to display relevant ads, but can also be used to create detailed profiles of users and collect personal information without their knowledge or consent.

Another issue is cross-tracking, in which algorithms use information collected from one website to display ads on other websites. This can result in a large number of unwanted ads and can invade users' privacy.

Moreover, machine learning techniques to adapt to users' changing preferences and behaviours can lead to the exposure of inappropriate or misleading content.

Meanwhile, some algorithms may be designed to display ads that are appealing to users, but in reality are misleading or even fraudulent, which can have a negative impact on the user experience and their perception of the brand.

Hence, digital advertising algorithms can invade users' privacy by collecting and using personal information without their knowledge or consent, which can lead to privacy, security and deception issues. It is important that companies and algorithm developers take steps to ensure that users' privacy is respected and protected.

3. Benefits of digital advertising vs. privacy risks

Digital advertising offers a variety of advantages that are not available with the use of more traditional advertising media, such as print or television.

To begin with, greater precision in targeting audiences. With digital advertising, advertisers can use demographic, behavioural and navigational data to create accurate target audience profiles, allowing them to reach a specific and relevant audience. For example, a baby clothing advertiser can segment its target audience through demographic data such as age and gender, and behavioural data such as search terms related to parenthood.

At the same time, it offers greater efficiency in advertising spending. Digital advertising enables accurate measurement of campaign performance, allowing advertisers to optimize their budget and maximize their return on investment. For example, with tracking and measurement tools, advertisers can measure the number of clicks, conversions and cost per conversion, and adjust their campaigns accordingly.

Higher flexibility as well. Digital marketing allows advertisers to change or adjust their campaigns in real time, allowing them to quickly adapt to trends and changes in consumer behaviour. An example would be when an advertiser notices that their ads are not generating enough clicks, they can change the design or content of their ads in a matter of minutes.

We also encounter increased reach. Digital advertising allows publishers to reach a global audience through the Internet. Through social networks, they can reach millions of people around the world. Online ads can also be displayed on websites and mobile apps, allowing advertisers to extend their reach to a wider audience.

Another important benefit is the greater capacity for measurement and analysis. Digital advertising allows advertisers to measure and analyse the performance of their campaigns in real time, enabling them to make adjustments and improvements to achieve better results. For example, advertisers can use analytics tools to measure the impact of their campaigns on social media, website traffic, conversion rates and ROI.

This allows them to evaluate the performance of their campaigns and make informed decisions on how to improve their advertising strategy in the future. In addition, data-driven digital advertising also allows advertisers to perform A/B and multivariate tests to compare different versions of their ads and determine which one is the most effective.

Lastly, as mentioned above, the ability to personalize ads. With the use of data, advertisers can better understand their customers and tailor ads to meet their needs and preferences. This can significantly improve the effectiveness of ads and increase conversion rates.

Despite all the advantages it offers, there are also privacy risks associated with digital advertising.

One of them is the collection and misuse of personal data. Advertisers and advertising platforms can collect a wealth of personal information about users, including their browsing history, searches, online purchases, and demographic data, and use it to target personalized advertising. However, this data can be misused or shared with third parties without the user's consent.

The lack of transparency means that users are often unaware that their data is being collected and used for advertising purposes, and have no clear way to opt out. In addition, data collected by advertisers and advertising platforms can be vulnerable to cyber-attacks, which could result in a breach of privacy and exposure of personal information.

We also fin the tracking of navigation. Advertisers and advertising platforms may use cookies and other technologies to track users' online browsing, allowing them to collect information about their interests and behaviours. This can result in an invasion of privacy and a sense of constant surveillance.

Location-based advertising uses geolocation data to display personalized ads to users based on their current location, which can be useful for advertisers, but it can also result in an invasion of privacy if users are not aware that their location data is being used.

Likewise, there is misleading advertising. Online advertisements can be misleading or even fraudulent and can direct users to websites that contain malware or attempt to steal personal information.

Adding to the above, there is a risk of polarization and influencing decision making. Personalized ads can lead to online polarization, as users only see content that confirms their previous opinions and they are not exposed to different perspectives. This can have an impact on users' decision making, as they may be

influenced by the advertising they see and not make decisions based on their own criteria.

Advertisers may also share information with third parties without users' knowledge for research purposes. This means that advertisers can share personal information with third parties to help them conduct research on user behaviour. This can be useful for users, as they can receive better products and services, but it can also be a privacy concern, as users have no control over who receives their information and how it is used.

But above all, a very important issue that not many people are aware of, is the misuse of data, which is considered illegal due to the violation of privacy and data protection regulations and laws, as well as the illegal nature of the transaction. Much data is obtained illegally and sold through unregulated channels, such as dark web sites and cybercriminal networks.

The information sold or obtained may include personal data, such as names, email addresses, credit card numbers or social security information, among others. This data can be used to commit cybercrime, such as identity theft, by opening credit accounts or applying for loans in someone else's name.

Credit card numbers and banking information can be used to commit financial crimes, such as the purchase of fraudulent goods and services or the diversion of funds from bank accounts. This personal data can also be used for unwanted tracking or unauthorized access to personal devices and accounts, or even for cyber-attacks such as the distribution of malware and ransomware.

All this is suddenly dangerous for individuals, as their personal data can be used to commit crimes and violate their privacy, with serious legal and financial consequences for the people who buy or use it. However, millions of people may not be aware of this potential use of their personal data, as it is done in a discreet and covert manner, making it difficult to detect and prevent, thus creating ethical problems.

In overview, while digital advertising offers several benefits in terms of reach, measurement, interaction, and flexibility, it also carries a number of risks to users' privacy and security. It is important that companies and algorithm developers take the necessary steps to ensure that users' privacy is protected and adopt ethical practices in digital advertising, using data only for legitimate purposes.

4. Responsibility of governments and advertisers

All this raises questions about the use of personal data. How do you ensure that users' personal data is not used for unauthorized purposes? How accurate are the profiles generated by algorithms? How do users ensure that their data is secure?

In fact, there is regulation in the use of data by governments, which varies by country or region. There are several legal and regulatory frameworks that seek to protect the privacy of citizens and regulate the use of data by governments and companies, to ensure that users' personal data is not used for unauthorized purposes.

In Europe, the most important regulation is the General Data Protection Regulation (GDPR), which came into force in May 2018. The GDPR establishes regulations for the collection, storage and use of personal data by companies and governments, and requires companies to obtain explicit consent from users before collecting and using their personal data. In addition, the GDPR establishes significant financial penalties for organizations that fail to comply with the regulations.

In the United States, there are several laws that regulate the use of data by governments, including the Children's Online Privacy Protection Act (COPPA) and the Consumer Data Privacy Protection Act (CCPA). COPPA focuses on protecting the privacy of children under the age of 13, while CCPA focuses on protecting the privacy of adult consumers.

In Asia, some countries such as China and South Korea have implemented data privacy regulations, and meanwhile, some countries such as India and Singapore are still working on it.

Despite the plethora of existing regulations, there are several reasons why it is argued that more regulations are needed in this area.

An important one is the constant change in technology. Technology is constantly evolving and governments and regulations often struggle to keep up with the latest trends and technologies and the new ways in which data is collected and used. It is important that regulations are regularly updated to adapt to changes in technology.

The aforementioned lack of transparency. Many times, companies and governments do not provide sufficient information on how they are using user data. It is important that there are regulations that oblige companies and governments to provide transparent information on the use of data.

Insufficient protection of individual rights and privacy must also be considered. Many current regulations do not provide sufficient protection for citizens' individual rights and focus on general issues such as privacy, but do not address specific problems related to government use of data.

As well, there is a lack of training for regulators, as many regulators are not adequately trained on current technologies and trends. It is important that training programs are put in place for regulators to ensure that they are up to date with the latest trends and technologies.

In addition, it can often be difficult to enforce existing regulations, especially if governments are unwilling to provide information or are not subject to adequate oversight.

There may be political disagreements about how individual rights should be protected in relation to government use of data, which may delay or prevent the implementation of adequate regulations.

It is also important that regulations are put in place to ensure the security of personal data, as cyber-attacks are becoming increasingly common and can result in the exposure of personal information. In addition, it is important to keep in mind that regulations must be applied in a fair and equitable manner, avoiding bias and discrimination.

Thus, while regulations exist to protect privacy and regulate the use of data by governments and businesses, it is important that more regulations are put in place to adapt to the constant changes in technology, ensure transparency, protect

individual rights, protect privacy, and empower regulators. In addition, it is important that current regulations are regularly updated to ensure that they remain effective in protecting individual rights and privacy.

However, it is not only the government that needs to act, but companies must also take responsibility. It is important that advertisers comply with applicable privacy regulations and protect consumers' privacy in a number of ways, in addition to complying with the regulations described above.

One of them is obtaining consent. Advertisers must obtain explicit consent from consumers before collecting and using their personal information. To do this they must be transparent, they must provide clear and transparent information about how they are using consumers' personal information and how consumers can control the use of their information.

They must focus on data protection. Advertisers should implement adequate security measures to protect consumers' personal information from cyber-attacks and other risks such as loss or theft. To protect this data, they can use various security mechanisms such as data encryption or authentication to ensure that only authorized persons have access to advertising data. As well as access control to limit who can access them and how they are used and regular backups to be able to recover them in case of loss or damage.

To do so, they must analyse the risks associated with the collection and use of their users' data and take measures to mitigate them by making use of protocols to act quickly in case of security breaches or privacy violations. For example, the use of monitoring and intrusion detection tools to detect and respond quickly to any unauthorized access attempts. In addition, users should have access to their data and information about how it is used, and should be alerted in the event of a security incident. These measures help ensure that users are aware of the security of their data.

Limiting the use of personal information is another important measure. Advertisers should limit the use of consumers' personal information to the purposes for which consent has been obtained and not use personal information for unauthorized purposes. In addition, they must delete consumers' personal information when it is no longer needed for the purposes for which consent was obtained.

In addition, they must respect users' preferences about the use of their personal information, including options to opt out of receiving personalized advertising. Failure to do so may result in a loss of consumer trust and loyalty.

Due to the great importance of this issue, Apple in its update to iOS 14 introduced a measure that revolutionized advertising on Facebook or Instagram: When downloading these applications on an Apple device with iOS 14 or higher, you can choose not to use your data for commercial purposes, which led to Facebook Ads to chaos. With this measure, the campaigns could not be carried out well, as more than 70% of the population with an iPhone could not access their data. However, Facebook did not allow it and designed other ways to track the traffic generated by its ads.

In summary, it is important that advertisers comply with applicable privacy regulations and take steps to protect consumers' privacy. To this end, it is essential to develop a culture of data use responsibility for data privacy and security. This means that all users must be aware of their responsibilities for data management,

including data collection, use, storage and protection. It also means that advertisers understand and respect data security standards, as well as regulators and laws that set limits on data collection and use. And the importance of maintaining data privacy and using data ethically and responsibly must be understood. This culture of responsible data use will help companies protect their data and users have greater privacy.

5. Conclusion

Digital advertising algorithms have provided a platform for the promotion and marketing of products and services. However, they have also created risks to consumers' privacy, especially if steps are not taken to protect their information. These risks include unwanted tracking, unauthorized collection of personal data and illegal use of data by third parties.

Therefore, it is important for governments to regulate the use of data and for advertisers to be responsible for protecting consumer privacy. This may include implementing ethical policies and practices, employee training, transparency and consumer education.

By developing a culture of data use accountability, organizations can ensure that personal data is used fairly and transparently, which will help build consumer trust and loyalty. In addition, ethical and legal compliance with privacy regulations will help prevent legal penalties and damage to a company's reputation. In the same way, consumers will be informed and aware of the possible use of their data and will be able to make the decision whether they want to share it or not.

In essence, it is necessary to focus even more on how personal data are used in advertising, since for the various reasons proposed above they can put at risk not only privacy, but also the security of users. To achieve this, it is essential that companies and governments work together to ensure adequate protection of individual rights, privacy and data security. This will help build trust and loyalty among consumers and prevent illegal use of data.

References

Cohen, J. N. (2018). Exploring echo-systems: how algorithms shape immersive media environments. *Journal of Media Literacy Education, 10(2),* 139-151.

Lomborg, S., & Kapsch, P. H. (2020). *Decoding algorithms. Media, Culture & Society, 42(5*), 745-761.

Andrews, L. (2019*). Public administration, public leadership and the construction of public value in the age of the algorithm and 'big data'. Public Administration, 97(2),* 296-310.

Jobs, C. G., Gilfoil, D. M., & Aukers, S. M. (2016). *How marketing organizations can benefit from big data advertising analytics. Academy of Marketing Studies Journal, 20(1),* 18.

Tiago, M. T. P. M. B., & Veríssimo, J. M. C. (2014). *Digital marketing and social media: Why bother? Business horizons, 57(6),* 703-708.

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). *Data-driven digital advertising: benefits and risks of online behavioral advertising. International Journal of Retail & Distribution Management, 49(7)*, 1089-1110.

Boerman, S. C., & Smit, E. G. (2022). *Advertising and privacy: an overview of past research and a research agenda. International Journal of Advertising,* 1-9.

Weber, R. H. (2015). *The digital future–A challenge for privacy? Computer Law & Security Review, 31(2),* 234-242.

Kim, G. H., Trimi, S., & Chung, J. H. (2014). *Big-data applications in the government sector. Communications of the ACM, 57(3)*, 78-85.

Bertot, J. C., & Choi, H. (2013, June). *Big data and e-government: issues, policies, and recommendations. In Proceedings of the 14th annual international conference on digital government research (pp. 1-10).*

Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009). *Advertising and consumer privacy. Journal of advertising, 38(4),* 51-61.

Nill, A., & Alberts, R. J. (2014). *Legal and ethical challenges of online behavioral targeting in advertising. Journal of current issues & research in advertising, 35(2),* 126-146.