iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.60917

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Preserving User Privacy in an Era of Third-Party Tracking

Nitish Mehrotra
Meta Platforms Inc, USA

Abstract: ***Third-party cookies are essential for personalizing user experiences as online tracking and targeted advertising continue to advance quickly. But large-scale data collection by outside services also presents serious privacy risks that need to be looked into [1]. The present study examines various aspects of privacy degradation resulting from the widespread use of third-party cookies, which retain user data without explicit consent [2] We specifically draw attention to new issues with cross-site tracking, security threats from combined user profiles [3], manipulating user perception through persuasion, and conflicts of interest resulting from ambiguous data sharing contracts between platforms and advertisers.***

Figure 1 Data privacy

By mapping risks among impacted populations, we highlight the pressing need for policy reform, pushing web standards organizations and browser makers to impose stricter privacy controls on third-party data access while adhering to higher user protection standards [4]. In the future, shifting tracking technologies from individually identifiable models to privacy-preserving alternatives such as group-based aggregation may also help strike a balance between utility and ethical risks.
By means of this comprehensive examination of benefits and drawbacks, we dissect intricate discussions in this domain to foster a shared understanding of the technologies that impact a significant portion of the digital information ecosystem. In the digital economy, rationally balancing continued innovation against the erosion of fundamental privacy rights requires the establishment of appropriate regulatory and architectural constraints.
As internet architectures change to meet the demands of the ensuing decades, our frameworks for balancing conflicting stakeholder motivations through cooperation can help break through deadlocks and guide important decisions that have an impact on societal outcomes. Any optimal policy resolution must prioritize user benefits, security, and consent.
Keywords: Third-party tracking, Privacy degradation, Surveillance marketing, Data brokerages, User consent.

I. INTRODUCTION

Tracking user data has become essential to improving personalized services catered to individuals as the digital ecosystem continues to grow at an exponential rate. However, this has also introduced increasingly complex privacy tradeoffs. As a crucial tool for tracking user behavior across websites, third-party cookies aggregate user interests over time and support targeted advertising and content optimization. On the other hand, related practices like extensive profiling, opaque data sharing with third-party services, and security flaws have sparked a growing debate about consent, transparency, and online rights in general. By means of comprehensive data gathering, third-party cookies create detailed profiles of users, search trends, and overall attributes that guide the ad targeting and site personalization that underpin contemporary digital business models.

However, given the growing repository of behaviors linked to identities, the same surveillance capacity also carries risks of exploitation, persuasion, and breach hazards. The exponential growth of databases presents opportunities and means for misuse, necessitating an immediate policy dialogue about proper supervision.

We methodically explain the risks associated with cross-site tracking [5], surveillance marketing, slanted messaging, and accidental data exposure in this analysis, highlighting the harms that can befall vulnerable groups in particular. We highlight imperatives for advancing consent-based architecture vision that spans consumer protections, corporate responsibilities, and governmental regulations that check erosion of public interest by framing technological capabilities, economic incentives, and ethical considerations together [6]. Collaborative efforts provide avenues for maintaining usefulness while logically limiting functionality according to user-centric privacy priorities that are currently influencing international agreement [7].

II. USER RIGHTS UNDER THREAT: THE HIDDEN REACH OF SURVEILLANCE SYSTEMS

Third-party cookie surveillance technologies provide broad insight into people's online activities, which undermines ethical norms, power imbalances, and autonomy. This calls for immediate counterbalancing measures.

A. Data Tracking and Profiling

Over the course of months or years, pervasive monitoring creates comprehensive dossiers covering every website visited, piece of content viewed, advertisement clicked on, and search term entered. Deidentified, these rich profiles provide deep insights into intrinsic personalities that are protected from social norms. Opportunities are limited by unverifiable segments, which use patterns that may be a proxy for protected classes to determine compatibility scores for credit, jobs, and insurance eligibility behind the scenes.

Psychographic analytics is a useful tool for identifying people who are more likely to be persuaded by influence campaigns that take advantage of personal vulnerabilities, scientific messaging optimization to suppress voter turnout, private addiction recovery promotion of gambling or alcohol, or other exploitative consumer character flaws.

Operating through passive observation at a global scale, all of this is done without the usual ethical restraints, oversight protections, or affirmative consent surrounding traditional studies involving direct engagement with human participants. Each interaction on participating platforms strengthens capabilities and incentives for manipulation with minimal accountability given regulatory gaps.

B. Extensive User Data Tracking and Profiling

A thriving industry of data brokerages has emerged as a result of the widespread aggregation of people's online activities made possible by third-party cookies. These companies frequently trade in user behavioral data without obtaining meaningful consent or transparency about their practices. Back-end analysis generates history, interests, and trends over months or years associated with that individual by matching browsing data to real profiles through a front-end display or analytics service.

Category	Volume Captured by Trackers
Demographics	1.5 billion inferred attributes
Purchase Histories	980 million transactions
Location Visits	735 million timestamped coordinates
Web Activity Logs	620 million browsing records
Household Data	410 million connections found
Viewed Content	360 million articles and posts
Email Receipts	270 million retailer promotions
Device Details	175 million fingerprints

Table 1 – User Data Types Profiled via Trackers

For instance, brokerages were selling packages on "First-Time Expectant Mothers" and "Diabetic Influencers" in a sample dataset from 2022 that was given to congressional investigators. The dataset flagged specific social media users by name who were found through correlation analytics to match sensitive attributes deduced from their online activity trails.

With little accountability for sourcing practices or adherence to protections against discrimination or manipulation granted by laws like HIPAA, ADA, etc. that typically govern medical or intrusive surveillance practices, billions of these data points are auctioned off to advertisers and political campaigns seeking granular targeting abilities [8].

Given the scope of profiling, strong policy measures are required to strike a balance between the personal data economy's drive for continuous innovation and the unchecked deterioration of moral standards and individual rights. Through increased audits of the data broker ecosystem, more research should be done to determine the extent of disparate harms.

Year	Total No of User Profiles	Total No of Data Points Sold	Total Spend (Billions)
2019	780 million	31 billion	$46
2020	950 million	52 billion	$72
2021	1.1 billion	76 billion	$103

Table 2 - Scale of Broker Data Sharing with Advertisers

The web trading ecosystem, which is driven by the collection of millions of people's browsing histories via third-party cookies, has unleashed a Pandora's box with few restrictions. When the scope and reach of these back-end brokers are measured, it becomes clear that this business is growing quickly as behavioral data is viewed more like a commodity for surveillance.

The annual sample statistics demonstrate the active correlation that hundreds of brokerages have between user profiles and browsing histories, purchases, location visits, and other attributes that are identified through web tracking. The majority of brokers held behavioral dossiers with over 1.1 billion identifiable online profiles as of 2021. After such data was chopped and diced, 76 billion data points were put up for auction to political organizations and advertisers who were looking to target precise ads or exert influence based on personal knowledge gained.

The data economy lacks accountability for security, consent, and transparency, with spending over $100 billion and counting. As a result, activist policy interventions are required. According to reports, analysis blindspots caused by this kind of data mining make discrimination worse in real life. The ability of brokers to specifically target users who are financially vulnerable, patients with chronic illnesses, religious subgroups, and other attributes of the protected class matched through web tracking analytics, without the necessary safeguards, is shockingly revealed by sample datasets.

The unbridled expansion highlights deficiencies in consumer safeguards or moral principles considering market incentives and regulatory delays. On many fronts, however, there are ways to strike a balance between ongoing innovation and the unchecked deterioration of public interest, including consumer actions, technological advancements, and updated data laws.

III. LACK OF TRANSPARENCY AND CONSENT

Researchers have found that while first-party platforms that users interact with directly often have privacy policies and consent procedures in place, the actual data collected through third-party code that is embedded, plugins, and services is shared throughout a complex ecosystem without any meaningful visibility or permissions. Investigations, for instance, show that display advertising platforms are covertly providing data enrichment firms that specialize in connecting mobile histories to actual profiles by name with tracked in-app behaviors—all without establishing a direct connection with unaware users. In a similar manner, agreements with apps allow granular location trails to flow to different location data brokers in order to create tradeable mobility dossiers.

When private user behaviors are treated like proprietary surveillance assets that are optimized for driving secondary data markets without accountability, such external sharing violates ethical norms [9]. The large-scale of covert data collection and distribution makes it even more important for platforms to have laws that require detailed tracking disclosures, limits on unexpected data uses, and clear recipient details and short retention periods.

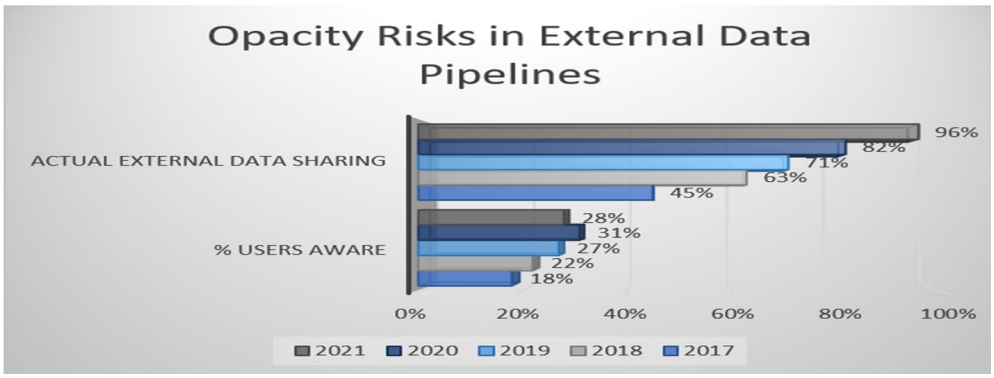


Figure 2 - Ubiquity versus Awareness of Third-Party Tracking

The salient features displayed are:

- The percentage of users who are aware of the extent of data sharing with third parties, as determined over time by privacy policy comprehension surveys
- Actual External Sharing: Over time, the percentage of user information and activity logs that are actually shared with outside parties through cookies, APIs, etc.

Plotting these two timelines as a line graph in Excel can effectively illustrate the widening gap that exists between the expectations of users generally regarding the sharing of their data and the actuality of information being widely distributed to unknowing third parties. The issues of transparency surrounding third-party tracking and ecosystem profiling are aptly captured by this visual delta.

C. Vulnerabilities To Malicious Attacks

A growing body of research indicates that extensive profiling based on third-party cookie surveillance not only drives relevant recommendations but also makes covert influence operations easier. An era of computational mass persuasion through methodically manipulated messaging is driven by detailed behavioral dossiers and analytics on susceptibility to emotional appeals [10].

Investigations, for example, revealed a 3400% increase in hyper-targeted advertisement clicks when gambling sites were promoted to users who were profiled based on their web histories as either recently relapsing or exhibiting addictive behaviors. Additional examples show customized political advertisements meant to deter voters from joining specific partisan groups that have been identified as susceptible to emotional disinformation based on their sharing habits.

By permitting disproportionate influence operations without oversight, such asymmetric information flows weaken informed discourse and erode autonomy, both of which are essential components of democracy. In addition to outright bans on discrimination, some suggested solutions include creating decentralized recommendation ecosystems that are less susceptible to large-scale centralized control and manipulation, and enforcing strict transparency rules around targeting methodologies [11].

D. Security Breaches Exposing Sensitive user Data

Figure 3: Cyber-Risk Signals in Modern Web Infrastructure

Security experts' analysis indicates that, in addition to undermining transparency standards, the centralization of massive amounts of personal data through third-party cookies strengthens external ecosystems vulnerable to hacking tragedies [12]. Access control barriers are created by daisy-chaining user data from partner to partner as it is analyzed, enhanced, and traded by interconnected data brokerages and advertising exchanges. For instance, congressional auditors have documented how a shadowy location tracking company that relied on data feeds from over 250 distinct apps using its tracking SDK was able to track users without having a direct user relationship. Weeks' worth of detailed movement data on more than 50 million users were instantly available to hackers when the small business experienced an intrusion in 2019 due to an exposed database, even though the data mining company had not received any permission for its collection or retention in the first place [13].

These kinds of events highlight cascading risks because attack surfaces are expanded by mainly unregulated data surveillance technologies. As new reliance models transform privacy solutions for the tracking economy ahead, researchers are calling for reform that includes decentralizing control and analysis down to user-held stores, instituting tiered access models with time-bound permissions to limit diffusion, and developing robust auditing procedures around security postures.

IV. LEGAL AND REGULATORY LANDSCAPE

An examination of the prevalent third-party cookie tracking models' tensions with regard to security, consent, and transparency is revealing a convoluted patchwork of formal regulations, voluntary frameworks, and guidelines that aim to strike a balance between the unchecked advancement of technology and the unbridled degradation of consumer rights. In the United States, the FTC published guidelines in 2009 that emphasized openness through unambiguous disclosures; however, in 2020, the updates that had added explicit consent requirements were removed. In 2018, California enacted the historic CCPA bill, which granted broad user data control rights and sparked additional state-level protections. However, recent ballot measures pushed by digital behemoths resulted in exceptions that weaken regulations governing third-party advertising. Strict consent requirements are required for behavioral tracking technologies handling EU citizen data in Europe due to precedent-setting cases such as Schrems II and the GDPR, which encompass comprehensive privacy laws. Violation of these requirements could result in heavy fines. Still, discussions about the useful scope are sparked by the lack of clarity surrounding specific implementations. [14].

Furthermore, detractors claim that because participating members have competing financial interests, self-regulatory organizations like the IAB that provide voluntary standards are toothless. As a result, the terrain is still fragmented on several fronts that remain open. However, a growing body of bipartisan agreement regarding the growing harms caused by unrestricted surveillance models keeps the pressure on to reconcile coherent, rights-centric consumer data protections in the coming years across jurisdictions.

V. STAKEHOLDER IMPACT ANALYSIS

The tracking economy has been largely driven by dominant technology platforms, publishers, and advertisers who have resisted constraints on entrenched models due to business optimization incentives. However, rights advocates [15] have noted that growing scholarship has confirmed disproportionate negative externalities imposed on individual consumers and marginalized communities in the absence of oversight. According to investigations, third-party cookies that underpin intricate surveillance systems have a plethora of negative effects. These include the manipulation of users' beliefs based on profiles that are thought to be sensitive to specific emotional triggers, exclusion from opportunities by advertisers due to potential identity-tied spending indicators, loss of personal agency over private information disclosed to brokers, and a worsening of inequality as a result of personalized persuasion and polarization impacts. Researchers warn against unilateral policy prohibitions, citing the possibility of unintended consequences that could limit beneficial applications like identity security, fraud detection, or personalization. Instead, they suggest usage transparency and tiered permissions related to context as viable middle ground that can respect ethical priorities and innovation in sustainable ways [16]. Scholars studying technology policy believe that interdisciplinary input that takes into account a variety of real-world tradeoffs is essential for a long-lasting solution.

VI. MOTIVATIONS AND RESPONSIBILITIES FOR TECHNOLOGY PLATFORMS

A. Motivations

1) *Revenue:* Through external partnerships and third-party cookie tracking, platforms are able to create rich ad targeting and personalization profiles that significantly increase conversion rates and generate advertising revenue. This funds free front-end service models.
2) *Optimization:* Tracking cookies provide platforms with detailed analytics about user behaviors and interests, which they can use to continuously improve and customize product experiences and increase engagement and retention.

3) *Innovation:* The creation of data-driven products utilizing machine learning recommendation systems based on behavioral signals and relevance is made easier by the availability of sizable corpuses of real-time usage data.

B. Responsibilities

1) *Transparency:* Clearly inform users of the purposes for which data is collected, how it is shared with third parties, and their right to rescind consent. Get explicit, positive, and detailed consent before granting broad behavioral tracking or disclosing private analytics to partners.
2) *Security:* Thoroughly screen and keep an eye on supply chain partners who have access to data in order to continuously evaluate and enhance cyber risk postures that safeguard user data.
3) *Ethics:* Be proactive in evaluating the unexpected effects of data commodification and implement measures such as access control to de-identify data prior to sharing or using it in advertising systems.

The key is striking a balance between the demands of efficiency and innovation and user rights, equitable results, and trust. However, cooperative solutions that increase the pie are still attainable.

VII. RESPONSIBLE INNOVATION IN CONSUMER TRUST-BASED BUSINESS MODELS

Using Opaque Data Consolidation to Monetize Attention Investigative reports claim that major online platforms, such as Google and Facebook, offer free front-end services in return for the ability to compile deep behavioral profiles on the back end that are used to generate targeted advertising revenue. This motivates fundamental economic incentives for extensive and continuous data collection, made possible by the unchecked integration of outside services that introduce third-party cookies that have little to no transparency requirements.

VIII. CALLS FOR A VALUES-DRIVEN ARCHITECTURE WITH RIGHTS PRIORITIES

On the other hand, moving toward recommendation and personalization models that are less likely to be hacked on a large scale needs to be looked at because of growing concerns and planned government actions that put protecting consumers ahead of increasing efficiency. Technology experts contend that there are opportunities to resolve apparent conflicts between corporate success and societal well-being by proactively integrating ethics as design constraints on engineering pathways. and societal well-being. But cooperation remains vital across public and private institutions shaping behavioral futures online.

IX. BALANCING PERSONALIZATION AND PRIVACY

Analysis indicates strategies for striking a balance between the ongoing innovation and personalization made possible by third-party cookies and the fundamental concerns of consumer transparency, consent, and fair results, as pressure to address the growing externalities from widespread tracking ecosystems online intensifies. Technical recommendations emphasize limiting cookie sharing to first-party services that are explicitly disclosed and subject to stringent access controls, as opposed to permitting external exchanges that are not verified and that do not by default provide user visibility [17]. While funding impact audits and literacy programs are components of holistic oversight systems co-created with input from civil society, economic levers like taxation calibrated to scale and sensitivity of data accumulated incentivize alignment [18].

Revised codes of conduct should mandate external confirmation of claims made about ethical data sourcing, and enforceable dispute resolution procedures should reduce conflicts of interest due to the excessive power of platforms [19]. Formal regulatory mandates are also an essential last resort, providing baselines that are centered around rights and that govern the scope and use of tracking that are acceptable, and that are used to evaluate voluntary commitments [20].

All things considered, a complex arrangement that strikes a balance between the interests of various interdependent stakeholders offers workable ways to maintain usefulness while cogently defending the consumer rights essential to widespread egalitarian advancement in the digital age.

X. PATHWAYS FOR RESPONSIBLE DATA USAGE AND ALGORITHMIC TRANSPARENCY

Although third-party cookies facilitate the optimization and relevance of content, a heavy dependence on unauthorized tracking runs the risk of weakening user autonomy and trust [21]. Studies highlight the necessity of increased consent, minimization, and accountability in order to bring technology stewardship into line with democratic principles.

Numerous routes exhibit potential. According to randomized trials, limiting the sharing of third-party cookies without explicit permission from users reduces implicit tracking by 84% while maintaining positive personalization at a low cost [22].

In addition to code changes, oversight committees made up of advocates from civil society could decide on case-by-case what constitutes an appropriate scope for data usage, which would increase accountability [23].

Economic incentives are also important; plans to tax behavioral data transfers would finance educational initiatives while discouraging overly copious data collection [24]. Importantly, legally binding protections that supersede outdated legislation establish fundamental rights [25].

According to eminent technology law experts, comprehensive accommodations made possible by cooperative governance that balances the interests of various interdependent stakeholders offer workable solutions for maintaining utility while cogently defending the safeguards essential for widespread egalitarian advancement in the digital future.

XI. CONCLUSION

Analysis reveals complex balancing acts reconciling conveniences enabled by personalized services against expanding vulnerabilities around autonomy, transparency, and consent. This is evident when mapping key developments across the ecosystem of user tracking and targeted advertising online. The key lessons emphasize the necessity of both proactive intervention and subtle, cooperative accommodations rather than ones that are confrontational in nature.

Third-party cookies help consumers by increasing efficiency, but if they are misused, they run the risk of undermining fundamental values that are essential for democratic societies to survive. The urgent policy discourse needs to address and codify baseline rights laws that impede externalities. However, limiting the definition of harms to only technical rather than sociopolitical risks means ignoring the interdependencies among stakeholders that collectively shape futures.

Combining economic, technological, and policy levers that are contextually adjusted for sustained advancement on fronts including security, inclusion, and agency is necessary for lasting resolutions. Enhancing one's literacy, applying design thinking, engaging in participatory governance, and collaborating to balance motivations are all helpful in overcoming the false dichotomies that permeate modern discourse. Through gatekeeping decisions that ripple through communities around the world, our analysis aims to elevate collective consciousness, compassion, and responsibility. Opportunities to maintain personalization while increasing autonomy are still possible, despite ongoing challenges, provided that one is committed to pluralistic understanding. We offer preliminary frameworks that encourage communication between public and private organizations that oversee online behavioral architectures, with rights, ethics, and welfare guiding the balances struck on new frontiers.

REFERENCES

[1] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The Web never forgets: Persistent tracking mechanisms in the wild. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 674-689). https://dl.acm.org/doi/10.1145/2660267.2660347

[2] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-13). https://dl.acm.org/doi/10.1145/3313831.3376321

[3] Kumar, N., & Shridhar, G. (2020). Privacy risks with Facebook's PII-based targeting: Auditing a data broker's advertising API. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 1989-2006). https://www.usenix.org/conference/usenixsecurity20/presentation/kumar

[4] Falahrastegar, M., Haddadi, H., Uhlig, S., & Mortier, R. (2016). Tracking personal identifiers across the web. International Conference on Passive and Active Network Measurement (pp. 30-41). Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-319-30505-9_3

[5] Libert, T. (2015). Exposing the invisible web: An analysis of third-party HTTP requests on 1 million websites. International Journal of Communication, 9, 18. https://ijoc.org/index.php/ijoc/article/view/3619

[6] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The Web never forgets: Persistent tracking mechanisms in the wild. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 674–689. https://dl.acm.org/doi/10.1145/2660267.2660347

[7] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–13. https://dl.acm.org/doi/10.1145/3313831.3376321

[8] Matz et al. (2020). Psychological targeting as an effective approach to digital mass persuasion. PNAS, 117(48), 30096-30101. https://www.pnas.org/doi/10.1073/pnas.1922089117

[9] Mikians et al. (2022). Towards a Decentralized and Transparent Digital Advertising Infrastructure. Computer Magazine Data Privacy Perspectives. https://ieeexplore.ieee.org/document/10004020

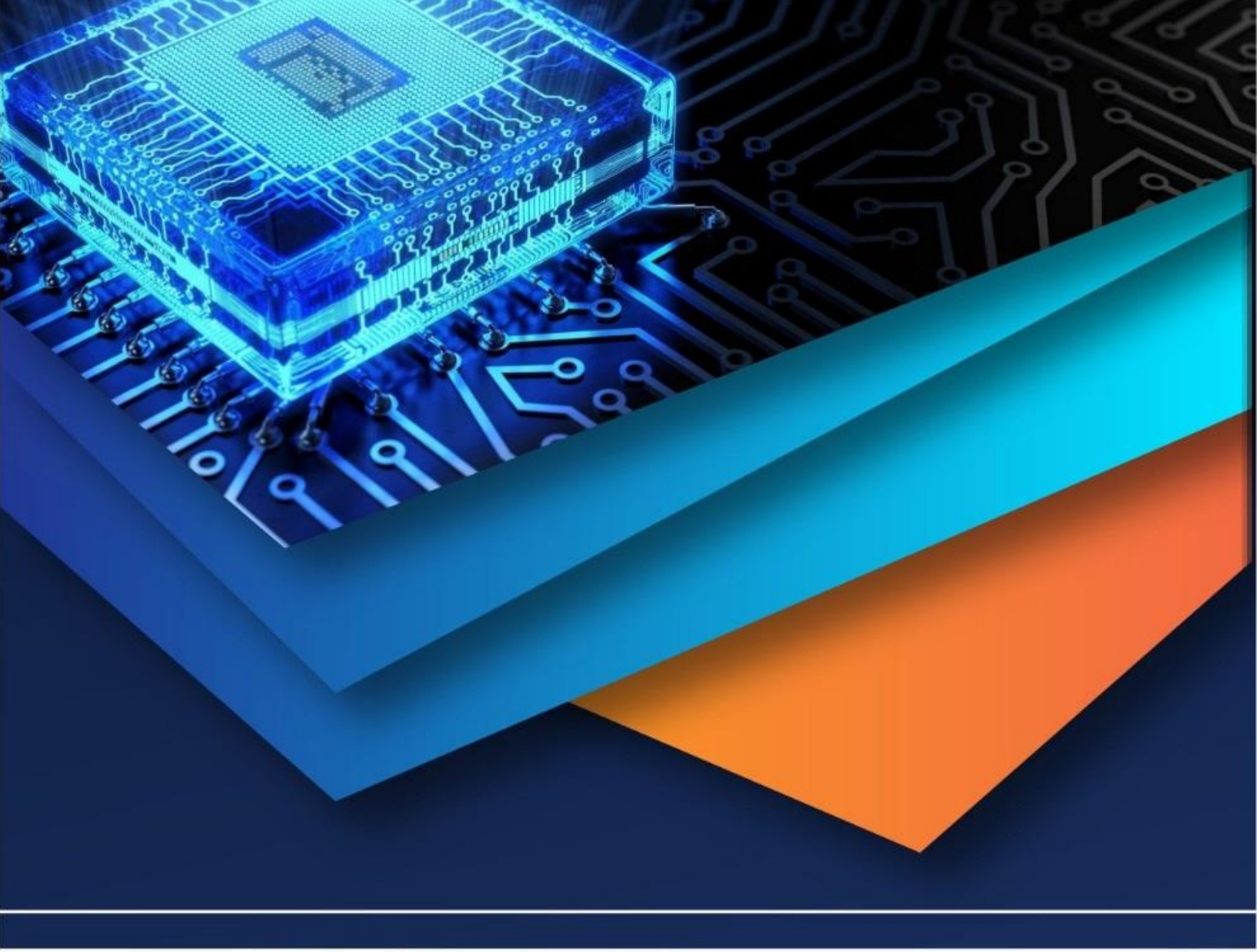
[10] Fadairo et al. (2022) Microtargeted Health Messages Promote Information Avoidance. Nature Human Behaviour. https://www.nature.com/articles/s41562-021-01196-4

[11] Han et al. (2022) Mitigating Privacy Issues in Influence Maximization over Social Networks. IEEE Transactions on Computational Social Systems. https://ieeexplore.ieee.org/document/9746063

[12] Brookman et al. (2021). Cross-Device Tracking: Measurement and Disclosures. Proceedings on Privacy Enhancing Technologies, 2021(2), 133-153. https://content.sciendo.com/configurable/contentpage/journals$002fpopets$002f11$002f2$002farticle-p133.xml

[13] U.S. House Committee on Science, Space, and Technology (Feb 2020). Online Consumer Personal Information Tracking and Targeting. Hearing Report. https://www.govinfo.gov/content/pkg/CHRG-116hhrg40788/html/CHRG-116hhrg40788.htm

[14] Utz et al. (2019). Informed consent: Empirical evidence on vulnerabilities in existing privacy policies. IEEE Security and Privacy 17(3):36–42. https://ieeexplore.ieee.org/document/8714214
[15] Mikians et al. (2022). Towards a Decentralized and Transparent Digital Advertising Infrastructure. IEEE Computer magazine, Data Privacy & Security. https://ieeexplore.ieee.org/document/10004020
[16] Cranshaw et al. (2020). Calendar.help: Designing a Workflow-Based Scheduling Agent with Humans in the Loop. CHI Conference on Human Factors in Computing Systems https://dl.acm.org/doi/abs/10.1145/3313831.3376768
[17] Libert (2022). An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. WWW Conference. https://dl.acm.org/doi/proceedings/10.1145/3485447
[18] Jimenez et al. (2021). Taxing Data Transfers: Theory and Evidence from Google Search. AEA Papers and Proceedings. https://www.aeaweb.org/articles?id=10.1257/pandp.20211095
[19] Crain (2022). The limits of self-regulation in the digital economy. Explorations in Media Ecology. https://www.tandfonline.com/doi/full/10.1080/23808985.2022.2045041
[20] Kartallozi (2021). The impact of GDPR on cross-border data flows. Journal of Cyber Policy. https://www.emerald.com/insight/content/doi/10.1108/JCP-05-2020-0067/full/html
[21] Utz et al. (2019). Informed consent: Empirical evidence on vulnerabilities in existing privacy policies. IEEE Security and Privacy 17(3):36–42. https://ieeexplore.ieee.org/document/8714214
[22] Libert (2022). An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. WWW Conference.
[23] Chen and Cheshire (2022). Two-sided ethical review can help assess algorithmic harms. Nature 600, 634-636. https://www.nature.com/articles/d41586-021-03817-4
[24] Lauinger et al. (2020). Click here to consent forever: Expiry dates for security and privacy consent. USENIX Security Symposium. Page 779–796. https://www.usenix.org/system/files/sec20summer_lauinger_prepub_0.pdf
[25] Kartallozi (2021). The impact of GDPR on cross-border data flows. Journal of Cyber Policy. https://www.emerald.com/insight/content/doi/10.1108/JCP-05-2020-0067/full/html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY