Digital Marketing in an Age of Privacy: The Intelligent Solution

Nirvikar Singh
Distinguished Professor of Economics
University of California, Santa Cruz
August 2021

FANPLAYR WHITEPAPER

Marketing in an Age of Privacy: The Intelligent Solution

Nirvikar Singh

Distinguished Professor of Economics

University of California, Santa Cruz

August 2021

1. Introduction

As the Internet and World Wide Web evolved, from research projects with ideals of free exchange of information to drivers of the 21st century global economy, fundamental contradictions began to emerge. Digital networks extend and amplify economies of scale, leading to the creation of commercial behemoths such as Alphabet, Amazon and Facebook. Companies like these are able to take advantage of vast troves of digital information about individuals, which they can gather at minimal cost. While an Amazon still relies on selling products and services to generate revenue,[1] an Alphabet or Facebook essentially makes its money – an enormous amount of it – from targeted digital marketing and advertising enabled by their platforms.

The problem is that the use of personal information by these companies, and by their marketing partners or subsidiaries,[2] grew by stealth, without user awareness or explicit permission. For some years, regulators struggled to deal with the problem of privacy violations, and the tech giants, especially in the United States, dealt with new laws by adopting confusing protocols for users to follow, typically requiring cumbersome opt-out measures. The tide began to turn in 2018, with the European Union's General Data Protection Regulation (GDPR), which is "the most important change in data privacy regulation in 20 years. The regulation will fundamentally

[1] Of course, for Amazon and other companies, these services now include renting their web infrastructure to other businesses.

[2] In a well-known example of cooperation becoming integration, Google, which was later renamed Alphabet, and was by far the dominant search engine platform, acquired DoubleClick, the leading digital advertising company at the time, in 2007.

reshape the way in which data is handled across every sector, from healthcare to banking and beyond."[3] Providers of web browsers and other tools for digital navigation are already adapting to the new situation, but there is a strong bias toward existing ways of doing business, which have often been cavalier about individual privacy. This challenge of reconciling the old with the new is laid out in the next section. After that, we present a specific solution that can take account of the existing infrastructure of digital marketing, while adding privacy protection. This solution combines digital tools from artificial intelligence and cryptography in an innovative manner. We conclude with a perspective on how this kind of approach, along with other innovations, can lead to a more balanced digital economy, one that respects both individuals and smaller companies more than is the case currently, while preserving many benefits of the existing digital marketing ecosystem.

2. Why is Privacy a Challenge?

Regulators around the world are enacting laws that make it easier for individuals to protect their privacy, especially personally identifiable information (PII). The EU's GDPR has been followed by similar efforts in major economies such as Japan and California, the most populous state in the US. As a result, even if the individual has to opt out rather than opt in, opportunities to do so are simpler, more transparent, and more manageable than before.

Companies that provide web browsers or other online navigation tools for individuals are also responding to new regulations, by creating enhanced methods for privacy control. In addition to responses to regulation, companies are also taking account of individual preferences, including an increased awareness of, and desire for, privacy

[3] This quote is from their website, eugdpr.org.

protection options.[4] Individuals can now protect their privacy much more easily while browsing online. They can prohibit certain kinds of data – the innocuously named, ubiquitous, "cookies" – from being collected and stored on a user's computer.

Some cookies are essential for functionality, allowing various pieces of Internet software to preserve continuity through a basic kind of tracking. Without this basic tracking, Internet browsing could not work, since information is stored in a very decentralized manner. Basic tracking allows software to create the needed bridges between various information storage sites for effective Internet browsing, as well as digital commerce. Other cookies, however, reveal data about browsing habits, and possibly a range of other individual decisions and characteristics, to whoever has access to the data. In particular, the digital advertising and marketing ecosystem has grown around the use of a whole range of "third-party" cookies, those which are deposited by advertising companies or other interested parties, such as platform providers, as an individual person moves around the Internet and Worldwide Web.

Third-party cookies support extensive tracking, as well as targeting individuals with tailored advertising or offers, across websites and over time. They can be, and are, collated with PII, making them the source of potential privacy violations in the absence of informed consent by individuals. At the same time, there can be significant benefits for companies and for consumers, when they help companies to customize product and service offerings (such as features and prices) for individual Internet users. Much of the consumer-facing digital economy has developed and grown around this "tracking and targeting" ecosystem, generating large profits for major platform providers like Alphabet and Facebook, in addition to creating more chances to satisfy consumer wants effectively. But this has come at a high cost in terms of personal privacy.

---

[4] A comprehensive survey of the academic literature on the role of data privacy in marketing is provided by Martin and Murphy (2017). They consider psychological, ethical, organizational and economic aspects of the issue, and how firms can be strategically proactive in responding to a combination of new regulations and changing consumer preferences. Naturally, the literature has continued to grow rapidly after the date of this survey, and example include explorations of regulatory developments (Rothstein and Tovino, 2019; Rustad and Konig, 2019; Pernot-Leplay, 2020), the value of privacy to consumers (Winegar and Sunstein, 2019), implications for retailing and retail pricing (Zuiderveen Borgesius and Poort, 2017; Martin and Palmatier, 2020), and impacts on the business model of tech giants that rely on collecting large amounts of data (Houser and Voss, 2018).

An important change that can be made is for online sellers and service providers to rely less on indiscriminate collection of potentially sensitive individual data from across the Internet, and more on developing a better understanding of users who are ready to engage with them online. Specifically, new artificial intelligence (AI) tools embodied in solutions such as the Fanplayr Behavioral Data Hub (Singh, 2019, 2020) and its associated software suite enable companies to respond intelligently in real-time to individual online behavior on their sites, without relying on PII, or on third-party data from elsewhere on the Internet.[5] This behavioral-data-centric approach has proven effectiveness, as measured by higher conversion rates and average order values.

At the same time, one cannot completely or immediately abandon the existing digital infrastructure for understanding and addressing customer wants. To do so could cause significant disruption in the digital economy, and perhaps even stifle promising innovations, such as "open banking," (KPMG, 2019), which aims to create ecosystems that integrate financial management with other aspects of consumer decision-making. The challenge is how to avoid this disruption while respecting privacy, both because this is what individuals want, and because governments are increasingly enshrining this preference in new laws and regulations. The next section describes how this seemingly impossible task can be accomplished – an intelligent solution to the new digital privacy challenge.

3. The Intelligent Solution: PrivacyID

The solution described in this section does not resurrect third-party or cross-site tracking. That is not a good fit with the new landscape of digital privacy. In the

---

[5] Singh, Sunkara and Yencken (2021) provide the following observations on behavioral data, "In the context of digital networks, behavioral data covers a range of possibilities: browsing characteristics such as total time on site, speed, page views, and exit intent, in addition to click patterns; interest in specific products and characteristics; visit outcomes; and records of previous visits, where possible, are all examples. As opposed to demographic data, behavioral data does not have to – but sometimes can – be tied to a specific individual. Indeed, 'personalization' in this context takes on an expanded meaning: 'personas' can be created based on repeated patterns of behavior, and used to guide responses. Responses to an individual customer need not be locked into templates dictated by their age, occupation, income, or even past behavior. Instead, 'personas' derived from behavioral data can be dynamic and flexible, reflecting changing moods and objectives."

current digital marketing ecosystem, third party services (such as Google Analytics) also handle first-party data specific to individual businesses' websites. However, their approach is not necessarily privacy-protecting, and the potential for data spreading elsewhere is always present.

Many of the third-party services that businesses use for analytics, marketing and personalization also have tools that identify returning visitors to a website. In this case, first-party data is able to persist across multiple visits to that website by the user. The method is based on generating random user IDs for visitors and storing this information in a browser cookie. But in response to new laws and increasing individual privacy concerns, browser software is imposing more and more limitations on cookies in the browser, reducing their lifespan and their usefulness for businesses in the digital realm.[6] Some third-party services do provide ways for website owners to associate their own user identities with the identity created by the service. This enables the user to be recognized even when their own cookies have been limited by the browser software.

PrivacyID, developed by Fanplayr, uses an approach that works on similar principles, but with a clearer focus on user privacy, allowing for a more robust solution to the challenge of balancing the goal of serving customers with their concerns for privacy protection. PrivacyID is able to persist user identities much longer than regular cookies. At the same time, it ensures compliance with evolving privacy standards as implemented in browser software. Specifically, PrivacyID does not permit tracking of users across different websites, nor does it track or store any sensitive user information that can be used to personally identify users (PII).

How is privacy-respecting identification achieved? In simple terms, PrivacyID integrates into a business's web server and assigns a unique, anonymous identifier to each visitor on the site. The persistent ID that is created is transformed using a secure one-way cryptographic hash before it is tracked, so it is never exposed

---

[6] According to Fanplayr CTO Rajiv Sunkara (personal communication, used with permission), "Every browser vendor has taken a different approach in their implementation of tracking prevention. One thing consistent between them is that they are all making it increasingly difficult to track a user's journey across sites."

outside of the company's own network, and PrivacyID itself has no way to determine the original value. In particular, PrivacyID does not itself capture, store or provide any data. There is no data exchange with other services, other than the already-encrypted user ID.

An important additional aspect of how PrivacyID works is that it generates a separate hash for each of the third-party services to which it is applied. This results in the provision of a different unique ID for each service-user combination. This ensures that the user ID is different for each service, but consistent across visits. Privacy is protected across different components of the digital ecosystem that so many online businesses rely on.

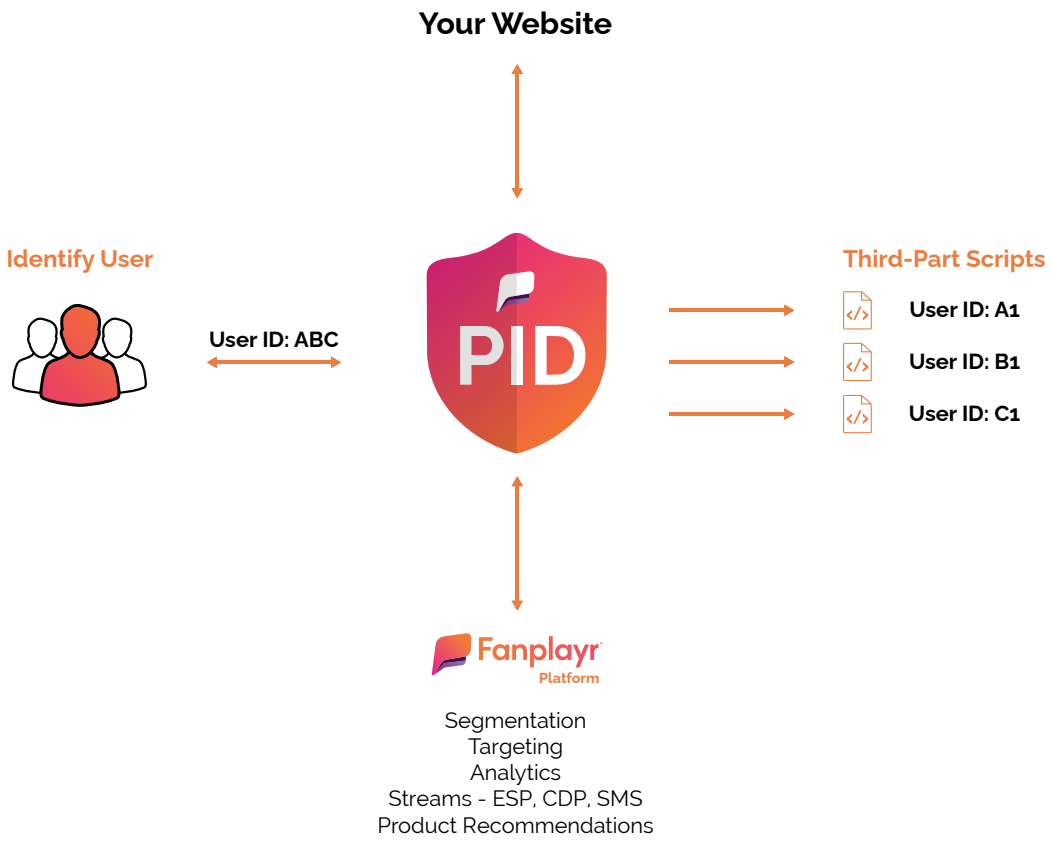
The privacy-respecting IDs created by PrivacyID can be a foundation for everything else a business chooses to do in the digital realm, including analytics, marketing and personalization. For example, the Fanplayr Behavioral Data Hub can be integrated with PrivacyID. But identities created by PrivacyID can simultaneously be shared with other third-party services to enhance their visitor recognition process and protect their typical business functions without compromising privacy. Newer services that evolve in approaches such as open banking can also take advantage of this simultaneous protection of functionality and privacy. In this sense, PrivacyID allows for innovation as well as avoiding disruption in the existing e-commerce ecosystem.

Using PrivacyID removes the need for additional integration steps with each third-party service, which can lead to significant savings in time and stress. Furthermore, it allows optional integration with management of consent categories for cookies (which types of cookies a user wants to allow, beyond those that are strictly necessary), as well as "right to be forgotten" requests based on Europe's Interactive Advertising Bureau Transparency & Consent Framework.[7] All of this can be controlled via a single dashboard, in essence, creating a Data Privacy Hub that lays a needed new foundation for digital commerce (see Figure 1).

---

[7] Such requests are forwarded to the relevant third parties, as they must be, and are not handled within the PrivacyID hub. However, website users have greater transparency and consistency with respect to how their privacy is being treated.

Figure 1: PrivacyID as Data Privacy Hub



Source: Based on Fanplayr documents

Ultimately, every company wants to serve its customers and clients more effectively, as a pathway to increased revenue and profits. Digital commerce has provided convenience and cost-savings for those customers and clients, but with increasing concerns about erosion of privacy. These concerns have led to a strong regulatory response. In an existing e-commerce ecosystem that has not done a good job of managing data privacy, PrivacyID represents an intelligent solution, because it works without disrupting the system, simply putting privacy management at the foundation of other services, while laying the groundwork for future innovation.

4. Conclusion: Toward A More Balanced Digital Economy

The evolution of digital commerce has seen the emergence of technology giants that benefit from the economies of scale inherent in their platforms and in the networks that use those platforms. There are increasing societal concerns about market power, which tilts the capture of value toward these giants, and away from individuals and smaller companies. These giants also have a scale advantage in the harvesting and use of individual data online, which further magnifies their market power. Ethical concerns about respecting individual privacy are therefore aligned with concerns about inequality in the new economy powered by digital technology. From multiple perspectives, the digital economy is unbalanced, and that needs to change.

At the same time, the ecosystem of digital technologies that has developed over time has many advantages. The increased use of behavioral data that is generated in the digital last mile on company websites (for example, with Fanplayr's Behavioral Data Hub) provides a more balanced approach to digital marketing than concentrating too many resources on driving traffic to the website. The AI approach to behavioral data enables more productive engagement with existing and potential customers, resulting in demonstrated benefits for performance measures like conversion rates and average order value. But an array of existing digital tools and third-party services still have important roles to play in digital marketing. The ability of these services to do their job will erode as reliable user identification becomes more difficult in a world of privacy restrictions. PrivacyID is conceived and engineered to ensure that reliable user identities can be created and managed simultaneously with innovative privacy protections. This combination of features allows company websites – and the services they rely on – to keep working, thereby protecting the quality of onsite user experiences, personalization, marketing and analytics that everyone has come to expect.

The COVID-19 pandemic has highlighted the importance of digital technology for the economy, and accelerated its role in our lives, beyond just commercial activities. Giving digital commerce new foundations that have greater privacy protection is

more important now than ever. The challenge is to do so while minimizing disruption of a digital ecosystem that has been built over decades. PrivacyID represents a significant contribution to the toolkit of solutions to this challenge.

Postscript: A Peek Under the Hood

Integration Steps

PrivacyID integrates into multiple layers of a company website to provide maximum compatibility with evolving browser privacy standards. Only two layers require integration via code (3 & 5) and one layer (4) via a network configuration. Once the solution has been integrated, simple JavaScript APIs can be invoked to provide user identifications services to third-party scripts (7).

1. ***PrivacyID Servers***

   Fanplayr's global infrastructure that powers PrivacyID.

2. ***Web Server***

   Company web server(s) which handle all requests for your website.

3. ***API Endpoint*** **(Integration Required)**

   A new endpoint on the web server will handle communication between the browser and the PrivacyID servers. It will also persist the user identity in a secure cookie which can only be accessed by company servers and is not visible to client-side JavaScript.

4. ***DNS Entry*** **(Integration Required)**

   A new CNAME DNS entry will point a subdomain of the company website to the PrivacyID servers. This will allow the full PrivacyID JavaScript Library (6) to be loaded through your domain to ensure that it maintains compatibility with browser privacy standards.

5. ***PrivacyID Embed Snippet*** **(Integration Required)**

   This JavaScript code will go on every page of the company website where users need to be identified. This snippet handles initialization of the PrivacyID library (6) and allows specification of the new endpoint (3) and subdomain (4).

6. ***PrivacyID Library***

   This handles communication with the new API endpoint (3) on the company web server and responds to third-party requests (7) for the user's identity.

7. ***Third-Party Clients*** **(Integration Required)**

   Each client and service that uses PrivacyID will obtain unique and consistent user identifiers by making simple requests to the PrivacyID JavaScript API.

User Interface

1. ***Dashboard***

   The PrivacyID dashboard gives insight into the usage of PrivacyID. The dashboard is made up of three graphs: the daily unique user count for the filtered site for specified dates and a breakdown into new and returning users.

2. ***Sites***

   The PrivacyID sites page in the Fanplayr portal allows users to manage sites associated with the PrivacyID feature. In order for a domain to have access to PrivacyID, the URL must be set up on this page. Different sites can reference the same URL. For example, there can be different sites for staging and production.

3. ***Scripts***

   PrivacyID scripts are created and managed on this page. Each script created can be attached to different sites independently. Similarly, the categories of each script are set per site. These settings can be managed in Setup (next bullet).

4. ***Setup***

   The setup screen is where scripts, sites, and categories are connected. The page has a section for each site set up on the Sites page. In each of these site sections, a user can attach or remove a script to the site.

References

Houser, Kimberly A. and W. Gregory Voss (2018), GDPR: The End of Google and Facebook Or a New Paradigm in Data Privacy, *Richmond Journal of Law & Technology*, 25(1): 1-70.

KPMG (2019), *The Future is Open: Reshaping the banking experience*, December, available at https://home.kpmg/xx/en/home/insights/2020/01/the-future-is-open.html.

Martin, Kelly D. and Patrick E. Murphy (2017), The Role of Data Privacy in Marketing, *Journal of the Academy of Marketing Science*, 45: 135–155.

Martin, Kelly D. and Robert W. Palmatier (2020), Data Privacy in Retail: Navigating Tensions and Directing Future Research, *Journal of Retailing*, 96(4): 449-457.

Pernot-Leplay, Emmanuel (2020), China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?, *Penn State Journal of Law & International Affairs*, 8(1): 49-117.

Rothstein, Mark A. and Stacey A. Tovino (2019), California Takes the Lead on Data Privacy Law, *The Hastings Center Report*, 49(5): 4-5.

Rustad, Michael L. and Thomas H. Koenig (2019), Towards a Global Data Privacy Standard, *Florida Law Review*, 71(2): 365-453.

Singh, Nirvikar (2019), The Digital Last Mile in E-Commerce: The Fanplayr Behavioral Data Hub, *Fanplayr Whitepaper*, December, available at https://fanplayr.com/files/whitepapers/Fanplayr_Whitepaper_2019.pdf.

Singh, Nirvikar (2020), Digital Commerce in the Post-COVID Network Age, *Fanplayr Whitepaper*, October, available at https://fanplayr.com/files/whitepapers/Digital Commerce Post-COVID - October 2020.pdf.

Singh, Nirvikar, Rajiv Sunkara and Simon Yencken (2021), Power, Privacy and Personalization in Digital Commerce, Working Paper, March, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3780726.

Winegar, Angela G. and Cass R. Sunstein (2019), How Much Is Data Privacy Worth? A Preliminary Investigation, *Journal of Consumer Policy*, 42: 425–440.

Zuiderveen Borgesius, Frederik and Joost Poort (2017), Online Price Discrimination and EU Data Privacy Law, *Journal of Consumer Policy*, 40: 347–366.