Access Partnership

Digital privacy reimagined:

The case for privacy-enhancing technologies (PETs) in Brazil and Mexico

August 2025

All information in this report is derived or estimated by Access Partnership analysis using both non-Google proprietary and publicly available information. Google has not supplied any additional data, nor does it endorse any estimates made in the report. Where information has been obtained from third-party sources and proprietary research, this is clearly referenced in the endnotes. With the exception of desktop research claims which have been footnoted, all claims in the report have been derived based on Access Partnership modeling.

About Access Partnership

Access Partnership makes innovation work for the world, guiding businesses and governments through complex regulatory challenges. It shapes regulations and policies that are fair and enable market access for innovative companies, drive growth, and attract investment into national markets. The firm's roster of world-leading clients includes the largest tech and innovation companies, major government bodies, and multilateral lenders and development organizations. Find out more here: accesspartnership.com.

Contents

Digital privacy reimagined: The case for privacy-enhancing technologies (PETs) in Brazil and Mexico

06 Executive Summary

08 Introduction

1.1. The rise of digital advertising in Latin America

1.2. The growing demand for privacy and data protection

1.3. The industry response: How advertisers and platforms are adapting

11 The importance of PETs in the digital ecosystem

2.1. Why PETs are a game-changer for digital advertisers

2.2 How PETs can drive value for advertisers in an evolving privacy landscape

16 Overcoming privacy challenges through PET adoption

3.1. PETs in action: Regional insights and global success stories

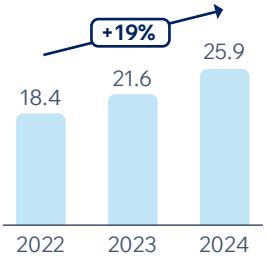
3.2. Breaking down adoption barriers: the role of industry collaboration

23 Conclusion

Digital advertising reimagined: The case for privacy-enhancing technologies (PETs) in Brazil and Mexico

Digital advertising is evolving in parallel with increased consumer awareness and demands to prioritize privacy.

Latin America is a fast-growing region with a burgeoning digital advertising market.



Annual digital advertising spend, Latin America

Consumers are increasingly recognizing the importance of their privacy and want their data to be kept safe.

"A company's data privacy policy affects whether I shop or use their services"[1]

Brazil: **80%**

Mexico: **88%**

% of respondents who agree

Businesses must adapt and are considering alternative advertising and data collection methods such as contextual advertising, first-party data strategies, or reducing the amount of data collected.

Among these, PETs stand out as a way for businesses to achieve **privacy-forward advertising,** where they safeguard privacy without compromising on data utility.

PETs are a crucial part of the digital ecosystem, and a key enabler to build trust among stakeholders.

While there is no universal definition for PETs, the term is used to refer to a broad set of technologies and methodologies designed to process and use data in a way that preserves privacy. These innovations enable data sharing and analysis without exposing personal information. Some examples include:

- **Differential privacy**, which adds noise to data to protect individual identities.
- **Trusted execution environments (TEEs)**, which ensure secure data processing within isolated environments.

PETs drive value for advertisers by:

- Strengthening consumer trust and brand reputation, especially as users become more privacy-conscious.
- Enabling personalized advertising with reduced privacy risks by minimizing direct data exposure.
- Supporting businesses, including smaller enterprises, in navigating compliance with Latin America's evolving privacy laws.

[1] Based on a survey of 2,551 consumers across Australia, Brazil, Germany, Mexico and the United Kingdom.
SOURCES: Statista (2024), IAB (2025), Access Partnership analysis.

There is potential for greater PET adoption in Latin America, with insights to be drawn from global successes.

Access Partnership analysis and interviews with data and privacy executives in the region (conducted in March and April 2025) have revealed that:

Privacy concerns are becoming a strategic priority, but **adoption and awareness of PETs remains uneven** across industries and business sizes. Sectors such as advertising and e-commerce tend to lead in this regard, and smaller firms face barriers such as **high relative costs and lack of technical expertise.**

While regulatory frameworks and consumer expectations are key motivators for firms, many remain **reactive rather than proactive**, with PET implementation being deprioritized in favor of short-term commercial goals.

Key roadblocks hindering adoption are **interoperability challenges** (such as differing regulatory frameworks), **practical cost considerations, and limited education on the topic**. An ongoing focus remains on effectively quantifying their return on investment, which highlights an opportunity for collaboration.

Moving forward, **stronger government support, collaboration among stakeholders such as advertisers, regulators and industry players, as well as greater clarity** on frameworks and regulations will be crucial to ensure more widespread and scalable PET adoption across the region.

Globally, PETs are already driving innovation and enabling valuable data analysis across various industries. Some examples include:

- Google's Confidential Matching product uses a PET called **TEEs**, which allows partners to securely connect and leverage their first-party data for effective audience management, in a way that balances privacy, security, and utility.
- A public-private coalition in the Netherlands developed a data analysis platform using **multi-party computation** to securely analyze elderly care data, enhancing policy insights while protecting sensitive information. The platform is currently being used in several regions, with intention to scale up nationally.

Facts about PETs

- Professionals recognize technologies such as differential privacy, but may not be familiar with the broader concept of PETs.
- PETs are not just standalone tools, but refer to a set of technologies and methodologies used to protect privacy while enabling data use.
- PETs can be integrated with existing digital ecosystems, such as applying homomorphic encryption for secure cloud computing.
- PETs alone do not guarantee privacy. They must be used correctly and responsibly, tailored to the specific context and privacy risk, and complemented with other enablers such as education and responsible data practices.

SOURCES: Google (2024), CoE-DSC (2023), Access Partnership analysis.

Executive Summary

Latin America is experiencing rapid digital transformation, driven by increased Internet adoption, smartphone penetration, and e-commerce growth, with Brazil and Mexico at the forefront. Digital advertising is a key driver of this transformation, with businesses shifting marketing budgets from traditional media to digital channels. Annual digital advertising spend in the region grew by 19% from 2022 to 2024, reflecting the increasing importance of online engagement on digital platforms.[1] This shift is supported by data-driven marketing, which offers benefits like real-time optimization, the ability to reach audiences more effectively, and detailed performance metrics. Notably, digital advertising democratizes market discovery by making customer outreach more scalable and affordable, empowering small and medium-sized businesses (SMBs) to compete more effectively and expand their reach in previously inaccessible ways through traditional advertising channels. This has generated significant returns on investment (ROI) for advertisers. For instance, a study by Access Partnership found that in 2023, the use of Google products such as Search, Ads, AdSense, Play, YouTube, and Cloud generated USD37 billion of impact for businesses in Brazil and USD15 billion in Mexico, of which a sizeable portion accrued to advertisers.[2]

However, concerns around data protection are increasingly shaping consumer behavior, alongside a growing awareness of data privacy laws in markets such as Brazil and Mexico. This comes on the back of an increasing number of incidents where data has been mishandled by companies.[3] In Brazil, 96% of consumers are familiar with their country's privacy regulations, while in Mexico, 85% share this awareness.[4] In response, advertisers are adapting by using privacy-friendly strategies, such as contextual advertising and first-party data, with big tech

platforms implementing privacy-enhancing initiatives.[5] Amidst this challenge of balancing privacy and personalization, privacy-enhancing technologies (PETs) are emerging as a way for businesses to collect and use data with privacy and security protections. PETs, which include innovations that facilitate data processing without compromising individual privacy, serve as key business enablers, allowing companies and public sector organizations to access, share, and analyze data that would otherwise be inaccessible.[6] They have broad applications, such as ensuring the security of financial transactions, supporting healthcare research and enabling privacy-preserving data analysis; however, this paper focuses on their role in delivering online advertising.[7] By integrating PETs, companies can strengthen protection of user privacy, comply with data protection regulations, and leverage data-driven insights while minimizing the risk of data breaches and maintaining consumer trust.

[1] Statista (2024), "Annual digital advertising spending in Latin America from 2022 to 2024". Available at: https://www.statista.com/statistics/1441302/annual-digital-ad-spend-latin-america/
[2] Access Partnership (2024), "Google's Economic Impact in Latin America". Available at: https://accesspartnership.com/googles-economic-impact-in-latin-america/
[3] Dark Reading, "Latin American Orgs Face 40% More Attacks Than Global Average". Available at: https://www.darkreading.com/cybersecurity-analytics/latin-american-orgs-more-cyberattacks-global-average
[4] IAB (2025), *Striking the Balance: The Consumer Perspective on Privacy, Preference, and Personalization.* Available at: https://www.iab.com/wp-content/uploads/2025/01/IAB_Consumer_Privacy_Report_January_2025.pdf
[5] Contextual advertising targets users based on the content they are viewing rather than personal data, while first-party data refers to information collected directly by a company from its users, such as website activity or purchase history, making it more privacy-compliant than third-party data.
[6] Sources include: CIPL (2025), *Privacy-Enhancing and Privacy-Preserving Technologies in AI: Enabling Data Use and Operationalizing Privacy by Design and Default.* Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_pets_and_ppts_in_ai_mar25.pdf ; and CIPL (2023), *Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age.* Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf
[7] Another term that commonly emerges in discussions is privacy preserving technologies, which focus on enabling data processing and analysis without exposing or compromising sensitive user information, ensuring compliance with privacy regulations while still allowing for meaningful insights.

In the context of advertising specifically, PETs are essential tools, enabling them to protect user data while still extracting valuable insights for digital marketing. These technologies and methodologies, like differential privacy—which adds statistical noise to data to maintain individual anonymity—and trusted execution environments—which create secure areas within processors to protect data during computation—allow for data analysis without compromising individual privacy. As digital advertising moves toward privacy-forward solutions, PETs play a key role in meeting increased user and regulatory expectations. For instance, Chrome's Privacy Sandbox includes tools that enable advertising measurement (such as attribution reporting), allowing businesses to assess campaign performance without tracking individuals across websites. By adopting PETs, advertisers not only align with privacy requirements but also build consumer trust, which is crucial in a market where privacy is a growing factor in purchasing decisions. In Brazil, 88% of people say that a company's data privacy policy affects whether they shop or use its services, while 80% of Mexican consumers feel the same.[8]

Through our analysis and in-depth interviews with data protection and privacy leaders across key sectors in Latin America, this report uncovers both challenges and opportunities in PET adoption. While businesses are increasingly prioritizing consumer privacy, adoption has not kept pace due to various difficulties. Key barriers include technical challenges and cost considerations. Moving forward, there is significant potential for PETs to drive competitive differentiation and enhance consumer trust across various industries. For businesses to fully realize the benefits of PETs, cross-industry collaboration is crucial, with stakeholders working together to share meaningful insights and drive collective progress. This will help foster confidence in PET deployment by ensuring companies understand how to implement these technologies in an effective manner. Accompanied by other enablers like strong data governance, clear frameworks, and industry standardization, PETs can be a key driver of privacy-forward innovation, allowing businesses to balance data-driven services with robust privacy protections.

[8] IAB (2025), *Striking the Balance: The Consumer Perspective on Privacy, Preference, and Personalization*. Available at: https://www.iab.com/wp-content/uploads/2025/01/IAB_Consumer_Privacy_Report_January_2025.pdf and/

1. Introduction

1.1. The rise of digital advertising in Latin America

Latin America is undergoing rapid digital transformation, fueled by rising Internet adoption, increasing smartphone penetration, and an expanding e-commerce ecosystem.[9] Brazil and Mexico, the region's two largest economies, are at the forefront of this shift, driving innovation in digital services, financial technology, and online marketplaces. As businesses and consumers embrace digital solutions at an unprecedented pace, the region is emerging as a key player in the global digital economy.

Between 2018 and 2023, the Internet penetration rate in Latin America grew from 65% to 81%, outlining the region's rapid digital expansion and increasing connectivity.[10] According to one estimate, in early 2025, Brazil boasted 183 million Internet users, representing an Internet penetration rate of over 86%, with Mexico following close behind at 83% (equivalent to 110 million Internet users).[11] Platforms such as Mercado Libre, which hosts over 100 million monthly active users, further bolster the region's digital ecosystem.[12] In Brazil, the success of Pix, an online payments method introduced by the Central Bank of Brazil, has revolutionized digital transactions, having facilitated digital payments for over 156 million individuals in the country.[13] This expanding digital landscape is unlocking new opportunities for businesses across the region.

1.1.1. Digital advertising is emerging as a cornerstone of the digital economy

Digital advertising has become a fundamental driver of business growth globally, enabling brands to reach consumers more efficiently and at scale.

Leveraging the rise in Internet penetration and usage, advertisers in Latin America are shifting their marketing budgets away from traditional media—such as television and print—toward digital channels. Across the region, annual digital advertising spend grew by 19% from 2022 to 2024, with businesses allocating over 40% of their media ad spend on digital advertising in 2024, making it the primary channel for advertising spend.[14] In Brazil, digital ad spend in 2024 (of USD8.7 billion) amounted to 56% of total ad spend. In Mexico, this figure was 61% (with a total digital ad spend of USD5.6 billion).[15]

1.1.2. Digital advertising is emerging as a cornerstone of the digital economy

Digital advertising offers businesses a multitude of benefits, including measurable insights, real-time campaign optimization, and to reach relevant audiences.[16] Unlike television or print ads, digital marketing provides detailed performance metrics

[9] Sources include: GSMA (2024), *The Mobile Economy Latin America 2024.* Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/latam/; EMarketer (2024), "Latin America E-commerce Forecast 2024". Available at: https://www.emarketer.com/content/latin-america-ecommerce-forecast-2024

[10] World Bank (n.d.), "Individuals using the Internet (% of population) - Latin America & Caribbean". https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2023&locations=ZJ&start=2018

[11] Sources include: Data Reportal (2025), "Digital 2025: Brazil". Available at: https://datareportal.com/reports/digital-2025-brazil; Data Reportal (2025), "Digital 2025: Mexico". Available at: https://datareportal.com/reports/digital-2025-mexico

[12] Statista (2025), "Number of active users of MercadoLibre, Inc. from 2022 to 2024, by vertical". Available at: https://www.statista.com/statistics/730433/mercadolibre-number-users/

[13] PCMI (2025), "Pix in Brazil: What to Expect in 2025 and beyond". Available at: https://paymentscmi.com/insights/pix-in-brazil-latest-statistics-central-bank/

[14] EMarketer (2024), "Latin America E-commerce Forecast 2024". Available at: https://www.emarketer.com/content/latin-america-ad-spending-2024

[15] EMarketer (2024), "Latin America E-commerce Forecast 2024". Available at: https://www.emarketer.com/content/latin-america-ad-spending-2024; EMarketer (2025), "Brazil leads regional growth in Americas ad spending". Available at: https://www.emarketer.com/content/brazil-leads-regional-growth-americas-ad-spending; and EMarketer (2024), "Mexico Ad Spending 2024". Available at: https://www.emarketer.com/content/mexico-ad-spending-2024

[16] Google (n.d.), "Benefits of online advertising and Google Ads". Available at: https://support.google.com/google-ads/answer/6123875?hl=en; and Adobe for Business (2023), "9 benefits of digital marketing". Available at: https://business.adobe.com/blog/basics/digital-marketing-benefits

such as click-through rates (i.e., the percentage of users who click on an ad or link after seeing it), conversion rates (i.e., the percentage of users who take a desired action), and engagement levels, allowing businesses to assess the effectiveness of their ad campaigns.[17] A study by Access Partnership found that in 2023, the use of Google products such as Search, Ads, AdSense, Play, YouTube, and Cloud generated USD37 billion of impact for businesses in Brazil and USD15 billion in Mexico, of which a sizeable portion accrued to advertisers. This outlines how digital advertising can drive revenue for businesses.[18]

Another key benefit of digital advertising is its flexibility. Marketers can adjust campaigns in real-time based on performance data, optimizing elements like ad creatives, target audience, and budget allocation.[19] This agility ensures that businesses maximize ROI and respond quickly to shifting consumer behaviors. Additionally, digital platforms enable precise audience segmentation, allowing brands to reach users based on demographics, interests, and online behaviors. With a population of 663 million people across Latin America, and cultural as well as linguistic diversity, this flexibility is particularly beneficial for advertisers in the region.[20] Digital advertising also plays a critical role across a wide range of industries, with sectors like retail, automotive, finance, and healthcare increasingly relying on digital channels to engage audiences, boost performance, and drive growth. For instance, in the context of Brazil, the retail sector leads in digital advertising, which comprises over 20% of its total online ad spending.[21]

1.2. The growing demand for privacy and data protection

With the evolution and growth of digital advertising, traditional advertising models have become increasingly reliant on extensive data collection to deliver targeted campaigns. However, consumers globally are becoming increasingly privacy-conscious and expect to engage with online content without the need to compromise their personal data. For instance, a survey conducted by Interactive Advertising Bureau (IAB) found that 88% of respondents in Brazil agreed that a company's data privacy policy affects whether they shop or use its services, while 80% of Mexican respondents feel the same.[22] Furthermore, in Brazil, 62% feel that their trust in how a company handles their data affects their purchasing decisions, underscoring how important it is for businesses to prioritize transparent data practices to maintain customer loyalty.[23] As digital commerce and advertising continue to expand in Latin America, companies that align with privacy expectations will gain a competitive edge, reinforcing the importance of ethical data use in an increasingly privacy-conscious market.

Consumers are also generally becoming more aware of the specific regulations that protect their privacy rights. For instance, 65% of respondents in Brazil highlighted that they are aware of the country's General Data Protection Law (LGPD),[24] suggesting that headline awareness of privacy issues is rising. This is likely due to the influence of policies like the LGPD and Mexico's Federal Law on the Protection of Personal Data held by Private Parties (LFPDPPP)[25], which resulted in more public discourse regarding data rights.[26] With consumers spending more time on digital platforms, their expectations for transparency and data protection are rising, placing growing pressures on businesses to adhere to stricter privacy standards and ensure clear data policies.

Though, it is also notable that educational efforts are truly important – only 39% in Brazil and 34% in Mexico are aware of how data protection laws affect their rights such as the ability to request the deletion of personal data. This also underscores the need for more targeted public education to help consumers understand how these regulations translate into real, actionable rights.

[17] Sources include: Google (n.d.), "Click through rate (CTR): Definition". Available at: https://support.google.com/google-ads/answer/2615875?hl=en. Google (n.d.), "Conversion rate: Definition." Available at: https://support.google.com/google-ads/answer/2684489?hl=en&sjid=6838075430639050337-NC

[18] Access Partnership (2024), "Google's Economic Impact in Latin America". Available at: https://accesspartnership.com/googles-economic-impact-in-latin-america/

[19] IMD (2025), How to start in Digital Marketing? A guide for 2025". Available at: https://www.imd.org/blog/marketing/digital-marketing/

[20] CEPAL (2024), "Population Growth in Latin America and the Caribbean Falls Below Expectations and Region's Total Population Reaches 663 Million in 2024". Available at: https://www.cepal.org/en/pressreleases/population-growth-latin-america-and-caribbean-falls-below-expectations-and-regions

[21] Statista (2024), "Leading digital advertiser sectors in Brazil in 2023, by share of online ad spending". Available at: https://www.statista.com/statistics/993282/digital-ad-spend-industry-brazil/

[22] Based on a survey of 2,551 consumers across Australia, Brazil, Germany, Mexico and the United Kingdom. Source: IAB (2025), *Striking the Balance: The Consumer Perspective on Privacy, Preference, and Personalization.* Available at: https://www.iab.com/wp-content/uploads/2025/01/IAB_Consumer_Privacy_Report_January_2025.pdf

[23] Access Partnership consumer survey of n=500 in Brazil, conducted in May 2025.

[24] Sources: ANPD (2018), *Brazilian Data Protection Law (LGPD).* Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf; and Access Partnership consumer survey of n=500 in Brazil, conducted in May 2025.

[25] Indesol (2016), "Ley Federal de Protección de Datos Personales en Posesión de los Particulares". Available at: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[26] A study conducted by the Interactive Advertising Bureau (IAB) reports that 96% of consumers in Brazil and 85% in Mexico are familiar with their country's privacy regulations. Source: IAB (2025), *Striking the Balance: The Consumer Perspective on Privacy, Preference, and Personalization.* Available at: https://www.iab.com/wp-content/uploads/2025/01/IAB_Consumer_Privacy_Report_January_2025.pdf

1.3. The industry response: How advertisers and platforms are adapting

Recognizing the growing consumer demand for stronger data protection, advertisers and digital platforms in Latin America are adapting their strategies to prioritize privacy. For instance, advertisers must now adapt to rising privacy concerns by embracing alternative advertising and data collection methods. Even without explicit restrictions on tracking being imposed, consumers have the choice to leverage options to refuse data sharing or opt out of personalized advertising altogether.[27] Such practices are becoming increasingly common in a landscape where consumer skepticism is higher, with only 38% of Brazilians feeling that they have sufficient control over their personal data online.[28] This has prompted some advertisers to turn to contextual advertising, which targets users based on the content they view rather than their personal data.[29] Additionally, first-party data strategies—where brands collect and use data directly from their customers—are becoming more prevalent.[30] AI-driven solutions, such as cohort-based advertising and anonymized insights, are also gaining traction, allowing businesses to reach audiences while minimizing personal data collection.[31] Meta, for instance, has tightened its data-sharing policies, limiting the amount of user information available to advertisers while enhancing privacy controls for consumers.[32] Similarly, Apple allows users to disable tracking requests from apps in their privacy settings, after which they will no longer receive prompts from apps that want to track their activity.[33] However, while minimizing data collection and relying on strategies such as first-party data and cohort-based advertising may help to ease user concerns, these changes come with trade-offs—without access to consumer data, businesses may face challenges in delivering relevant ads, leading to less effective marketing campaigns and potential revenue loss. This could compromise user experiences as consumers receive online experiences that are less tailored to their interests, affecting commercial viability.[34]

As such, advertisers must shift toward privacy-centric advertising by introducing new frameworks that balance data protection without compromising personalization. Concepts such as PETs have emerged as key to this shift. PETs employ methods like differential privacy, federated learning, and secure multi-party computation to allow advertisers to deliver personalized content and advertisements while protecting individual privacy.[35] They are essential tools in creating a more privacy-conscious advertising ecosystem, empowering businesses to continue engaging users effectively while safeguarding their personal data.

27 McKinsey (2020), "The consumer-data opportunity and the privacy imperative." Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

28 Access Partnership consumer survey of n=500 in Brazil, conducted in May 2025.

29 Google (n.d.), "Contextual Targetting". Available at: https://support.google.com/google-ads/answer/1726458?hl=en

30 BCG (2023), "First-Party Data Is Retail's Next Growth Engine". Available at: https://www.bcg.com/publications/2023/first-party-data-leads-next-growth-engine-in-retail

31 Sources include: SEO.AI (n.d.), "Federated Learning of Cohorts (FLoC)". Available at: https://seo.ai/faq/federated-learning-of-cohorts-floc; International Journal of Research in Marketing (2019), *Marketing analytics using anonymized and fragmented tracking data.* Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167811618300557

32 https://www.facebook.com/privacy/policy/

33 Apple (n.d.), "If an app asks to track your activity". Available at: https://support.apple.com/en-lamr/102420

34 International Journal of Research in Marketing (2023), *How has data-driven marketing evolved: Challenges and opportunities with emerging technologies.* Available at: https://www.sciencedirect.com/science/article/pii/S2667096823000496

35 OECD (2023), *Emerging privacy-enhancing technologies.* Available at: https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html

2. The importance of PETs in the digital ecosystem

2.1. Why PETs are a game-changer for digital advertisers

PETs do not have a single, universally accepted definition. Instead, the term encompasses a broad set of technologies and methodologies designed to protect user data while enabling useful insights and services. Different stakeholders, including regulators, academics, and industry players, define PETs based on their specific objectives.[36] For instance, a 2002 OECD (Organization for Economic Cooperation and Development) report defines PETs as a wide range of technologies that protect personal privacy, empowering users seeking to control the disclosure, use, and distribution of their personal information.[37] On another hand, the International Organization of Standardization (ISO) defines PETs as a privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system.[38] Despite these variations, all PETs share a common goal: to strike a balance between data utility and privacy protection, ensuring that businesses, governments, and users can benefit from data-driven innovations without compromising security.

For the purposes of this study specifically, PETs are defined as a wide range of technologies that help protect personal privacy while preserving data utility. These include tools that provide anonymity, as well as mechanisms that allow users to control if, when and under what conditions their personal information is disclosed. By empowering individuals with greater control over their data, PETs enable informed decision-making about how personal

information is stored, processed, and used. Common types of PETs and their applications are highlighted in Box 1 below.

It is also interesting to note that there is no correct way to categorize PETs, with sources offering varying potential categorizations for consideration. Some examples include:

- **OECD:** Groups PETs into four broad categories based on their function: (i) data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools. Most PETs can fit into more than one category but are assigned to a main category based on their primary function.[39]
- **Centre for Information Policy Leadership (CIPL):** Separates PETs into three categories: (i) cryptographic tools, (ii) distributed analytics tools, and (iii) tools for pseudonymization and anonymization.[40]

36 OECD (2023), Emerging privacy-enhancing technologies. Available at: https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html
37 OECD (2023), Emerging privacy-enhancing technologies. Available at: https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html
38 International Organization for Standardization (2024), "Information technology — Security techniques — Privacy framework". Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-2:v1:en
39 OECD (2023), Emerging privacy-enhancing technologies. Available at: https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html
40 CIPL (2023), Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf

- **Future of Privacy Forum:** Recognizes the PET categorization of input privacy (which refers to methods to mitigate unauthorized access or inappropriate use) and output privacy (which relate to methods used to minimize risks of re-identification in data analysis results or products).[41]

In digital advertising, PETs are crucial in strengthening data protection without introducing unnecessary friction for users (which refer to disruptions to user experiences such as intrusive data verification).[42] Combined with strong data governance, they enable advertisers to extract valuable insights, improve campaign effectiveness, and personalize user experiences, addressing growing consumer demands. PETs can also be integrated with existing digital ecosystems—for instance, applying homomorphic encryption to enable secure cloud computing without exposing sensitive information. More broadly, as highlighted in Chapter 1, effective use of PETs is essential to sustaining trust in the digital economy, enabling secure data-driven transactions and continued sector-wide innovation.

Box 1: Common types of PETs and their applications

While PETs differ in technical implementation, they serve a common goal: enabling businesses to extract value from data while protecting user privacy. The table below provides an overview of key PETs and their applications in advertising.[43]

Type of PET	Description	How it protects privacy	Applications in advertising
Differential privacy[44]	Adds statistical noise to data sets to prevent individual identification	Additional data is added to the core dataset before sharing to reduce the risk of a machine learning (ML) model memorizing user data or individual users	Enables aggregated audience insights without revealing individual user data
Secure multi-party computation	Allows multiple parties to analyze encrypted data without revealing individual inputs	Data is encrypted and cannot be deciphered without a key. This process is end-to-end, resulting in neither party seeing the other's data within trusted servers	Facilitates fraud detection and secure data collaboration between advertisers and partners
Homomorphic encryption[45]	Allows computations on encrypted data without decrypting it	Only the owner of the encryption key is able to see original data	Allows brands to analyze a platform partner's data while keeping user data private

41 Future of Privacy Forum (2025), "Privacy Enhancing Technologies: A State Education Agency Landscape Analysis". Available at: https://fpf.org/wp-content/uploads/2025/03/Privacy-Enhancing-Technologies-An-Education-Landscape-Analysis.docx.pdf

42 Deloitte (n.d.), "Privacy-Enhancing Technologies in Ad Tech". Available at: https://www2.deloitte.com/us/en/pages/chief-marketing-officer/articles/a-marketers-guide-to-privacy-enhancing-technologies.html

43 Note that many PETs fit into multiple categories, hence the list below should not be taken to be discrete. Sources include: Decentriq (n.d.), "What are privacy enhancing technologies?". Available at: https://www.decentriq.com/article/what-are-privacy-enhancing-technologies; Deloitte (n.d.), "Privacy-Enhancing Technologies in Ad Tech". Available at: https://www2.deloitte.com/us/en/pages/chief-marketing-officer/articles/a-marketers-guide-to-privacy-enhancing-technologies.html

44 With the use of differential privacy, privacy losses are quantifiable and can be measured using parameters like epsilon (ε) and delta (δ), which quantify the risk of an individual's data being revealed when using a differentially private algorithm. This can help advertisers balance personalization and privacy by setting measurable privacy thresholds, optimize the amount of noise added to datasets, and provide regulators and consumers with transparent assurances about data protection practices. Source: Harvard University (n.d.), "Harvard University Privacy Tools Project". Available at: https://privacytools.seas.harvard.edu/differential-privacy

45 It is important to note that in the context of digital advertising, applications of this technology are still fairly nascent and have yet to be explored extensively.

Type of PET	Description	How it protects privacy	Applications in advertising
On-device processing	Ensures user data is processed locally on a device rather than transmitted to external servers	Data never leaves the user's device, reducing the risk of interception, misuse, or unauthorized access	Supports contextual advertising without tracking user behavior across sites
K-anonymity	Groups users into cohorts to prevent individual identification	Data sets are grouped and layered, so that no individual data set is distinguishable	Used in audience segmentation to provide insights without exposing individual identities
Trusted execution environments (TEE)	Provides an isolated computing environment that allows data processing without exposing it to external parties	Unauthorized entities from outside the TEE are prevented from altering data, while code integrity prevents code from being replaced or modified by unauthorized entities	Allows for ad targeting and measurement while protecting sensitive data and preventing data alterations
Data accountability tools	Track, log, and audit how personal data is accessed, processed, or shared	Provide transparency and control by recording data flows and enabling enforcement of access permissions and policies	Help advertisers demonstrate compliance with privacy rules, manage user consent, and track data usage across vendors

2.2. How PETs can drive value for advertisers in an evolving privacy landscape

The digital advertising landscape is undergoing a significant transformation, moving towards a more privacy-centric model. Traditional digital advertising has relied on methods like persistent identifiers to track user behavior across websites and applications. However, growing privacy concerns have driven a shift away from these practices.

This industry-wide movement towards greater user privacy has spurred significant innovation in user-centric data approaches. A focus is increasingly being placed on developing and deploying privacy-forward solutions that can strike a more appropriate balance between individual privacy expectations and the utility required for effective advertising. For instance, Google recently announced that Chrome would enhance tracking protections, especially in Incognito mode, with the aim of launching IP Protection, a feature designed to obscure users' IP addresses from websites and trackers, making it harder to identify and profile individuals online.[46] These efforts aim to establish a sustainable and competitive digital advertising ecosystem that prioritizes user privacy while enabling publishers to fund content and businesses to connect with relevant audiences through novel, privacy-enhancing technologies.

In this new environment, PETs are critical enablers. As highlighted above, PET-based platform technologies such as Chrome's Privacy Sandbox offer practical, scalable ways for advertisers to continue delivering personalized, effective advertising without exposing sensitive user data. In the context of digital advertising, PETs are being

[46] Privacy Sandbox (2025), "Next steps for Privacy Sandbox and tracking protections in Chrome". Available at: https://privacysandbox.com/news/privacy-sandbox-next-steps/

increasingly recognized as tools that can be used to balance privacy with performance.

2.2.1. Enabling personalized advertising with reduced privacy risks

Amidst growing privacy concerns and regulatory shifts, traditional methods such as the tracking of users across apps and websites have become increasingly untenable. PETs revolutionize targeted advertising by allowing advertisers to deliver relevant content based on user interests without resorting to individual tracking. This offers a viable path forward for advertisers, enabling personalization without compromising user privacy.[47]

Such approaches ensure that advertisers are able to continue delivering ads that are relevant and engaging to consumers while still adhering to privacy-forward principles. Businesses can maintain advertising effectiveness while addressing consumer concerns, ultimately fostering a digital ecosystem that respects user privacy. The adoption of PETs can not only help advertisers navigate the limitations imposed by constraints of privacy regulations, but also foster greater user trust by demonstrating a commitment to data protection. As the industry continues to grapple with the balance between personalization and privacy, PETs are increasingly being recognized and invested in as fundamental building blocks for a sustainable and responsible digital advertising ecosystem.

2.2.2 Ensuring compliance with Latin America's evolving privacy laws

Latin America's regulatory landscape is undergoing rapid transformation, with countries enacting data protection laws inspired by global frameworks such as the European Union (EU)'s General Data Protection Regulation (GDPR).[48] In Brazil, LGPD imposes stringent requirements on data processing, while Mexico's LFPDPPP governs data collection and sharing.[49] Similar legislative efforts are emerging across the region, potentially increasing the compliance burden on advertisers who rely on personal data to reach the right audiences.[50]

PETs provide a way to navigate this by enabling advertisers to implement privacy-by-design principles that minimize the risk of data breaches and regulatory penalties. By integrating PETs, advertisers can align with legal requirements while continuing to leverage data for effective marketing.[51] This proactive approach can also help to highlight firms' commitment to ethical data practices, building trust with regulators and consumers.

2.2.3. Strengthening consumer trust and brand reputation

Consumer trust has become a competitive differentiator in digital advertising, with users increasingly aware of how their data is collected and used. As highlighted by a 2024 survey conducted by the Interactive Advertising Bureau (IAB), over 80% of consumers in Brazil and Mexico agree that a company's data privacy policy influences whether they shop or use their services, and more than 60% have stopped using a company's services because of their data-sharing policies and practices.[52] This highlights that consumers are becoming increasingly selective about the brands they engage with, making privacy a key factor in purchasing decisions. As such, advertisers that prioritize privacy stand to gain a significant advantage. PETs help build this trust by protecting personal data, reinforcing a brand's commitment to user privacy.

By adopting PETs, advertisers align with evolving privacy expectations and demonstrate a commitment to ethical data practices, enhancing customer loyalty and strengthening brand reputation in an increasingly privacy-conscious market.[53]

47 Decentriq (n.d.), "What are privacy enhancing technologies?". Available at: https://www.decentriq.com/article/what-are-privacy-enhancing-technologies

48 IAPP (2021), "3 years in, GDPR highlights privacy in global landscape". Available at: https://iapp.org/news/a/three-years-in-gdpr-highlights-privacy-in-global-landscape

49 Sources include: IAPP (2020), "Brazilian General Data Protection Law (LGPD, English translation)". Available at: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/; ANPD (2018), *Brazilian Data Protection Law (LGPD)*. Available at: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

50 Crowell (2025), "Latin American Data Privacy". Available at: https://www.crowell.com/en/insights/publications/latin-american-data-privacy

51 DSCI (2024), "Privacy-Enhancing Technologies: Global and Cross-Sectoral Regulatory Insights", Available at: https://www.dsci.in/resource/content/privacy-enhancing-technologies

52 Based on a survey of 2,551 consumers across Australia, Brazil, Germany, Mexico and the United Kingdom. Source: IAB (2025), *Striking the Balance: The Consumer Perspective on Privacy, Preference, and Personalization.* Available at: https://www.iab.com/insights/the-consumer-perspective-on-privacy-preference-and-personalization/

53 OECD (2023), "Emerging privacy-enhancing technologies". Available at: https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html

Box 2: Limitations of PETs

While PETs enable data to be analyzed or shared in ways that aim to protect user privacy, several technical and operational limitations still hinder their broader adoption and effectiveness:

1. Performance and scalability constraints

Technologies such as homomorphic encryption, secure multi-party computation, and TEEs can be resource intensive. They often result in high latency, increased infrastructure costs, and challenges scaling to environments that require rapid or large-scale data processing, such as digital advertising.[54] These barriers are especially high for small and mid-sized businesses.

2. Complexity and integration challenges

Many PETs require specialized expertise in areas like cryptography or data science. Integrating them may involve overhauling existing systems or creating custom solutions, which can be daunting for organizations without dedicated privacy engineering teams or technical infrastructure.[55]

3. Limited fit for certain use cases

Some applications may not be able to support PETs, making them difficult to implement.[56] Examples include:

- Delivering highly personalized content in real-time
- Tracking across devices and platforms without shared identifiers

This could create high barriers to entry and limit adoption, particularly among less digitally mature organizations.

4. PETs are not a substitute for good governance

While PETs can help limit data exposure, they must be part of a broader approach that includes strong internal policies, transparent external policies, and regular risk assessments. Without these safeguards, PETs alone cannot ensure responsible data handling.

54 ISACA (2024), "Exploring Practical Considerations and Applications for Privacy Enhancing Technologies". Available at: https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies

55 Qinshift (2024), "Privacy-Enhancing Technologies: The Benefits and Challenges for Tech Giants". Available at: https://qinshift.com/insights/techtopics/2024/privacy-enhancing-technologies-the-benefits-and-challenges-for-tech-giants/

56 ISACA (2024), "Exploring Practical Considerations and Applications for Privacy Enhancing Technologies". Available at: https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies

3. Overcoming privacy challenges through PET adoption

3.1. PETs in action: Regional insights and global success stories

PETs are increasingly recognized for their role in strengthening privacy protections across various industries, including retail, finance, healthcare, and e-commerce. In the context of digital advertising across these industries, PETs provide a foundation for privacy-forward personalization, secure data collaboration, and regulatory compliance, ensuring that businesses can maintain relevance while respecting user privacy. Global policy efforts for the adoption of PETs have included the release of guidance, the creation of sandboxes, and increased investment in PETs research and development, with the emergence of several successful use cases in recent years.[57] In Latin America specifically, efforts have been made to keep pace with global developments, with regulators discussing the potential of PETs to help mitigate privacy risks and reduce the identifiability of data.[58]

3.1.1 The state of PET adoption in Latin America

PET adoption in the region appears to be in fairly nascent stages. For instance, in Brazil, companies reported low familiarity with PETs, especially more advanced ones. Encouragingly, 80% of Brazilian companies highlighted that they were already using some form of traditional PETs, such as anonymization, although understanding and adoption of advanced PETs (such as secure multi-party computation) was said to be much lower.[59] One example is Mercado Libre, the leading e-commerce platform in the region with over 100 million active users. The platform has been actively involved in the research and implementation of privacy-preserving methods, including through the testing of Chrome's Privacy Sandbox APIs, helping to ensure their properties function as expected and

continue to give users a positive experience.[60]

To this end, governments are taking steps to encourage the innovation and uptake of the technology through various avenues. For instance, Brazil's Data Protection Authority, or Autoridade Nacional de Proteção de Dados (ANPD) recently conducted technical studies on anonymization and pseudonymization as a basis for its forthcoming guidance.[61] Such initiatives will be pivotal in shaping the course of PET adoption in the coming years.

3.1.2 Global PET success stories

Across the rest of the world, PETs are already unlocking significant benefits in a variety of ways. Some examples of emerging PET applications include secure multi-party computation used in cross-company data collaboration, differential privacy for anonymized audience insights, and federated learning for personalized ads without individual tracking. These technologies are being piloted by companies in sectors such as finance and

[57] FPF (2024), "CPDP LatAm 2024: What is Top of Mind in Latin American Data Protection and Privacy? From data sovereignty, to PETs". Available at: https://fpf.org/blog/cpdp-latam-2024-what-is-top-of-mind-in-latin-american-data-protection-and-privacy-from-data-sovereignty-to-pets/

[58] FPF (2024), "CPDP LatAm 2024: What is Top of Mind in Latin American Data Protection and Privacy? From data sovereignty, to PETs". Available at: https://fpf.org/blog/cpdp-latam-2024-what-is-top-of-mind-in-latin-american-data-protection-and-privacy-from-data-sovereignty-to-pets/

[59] Basic PETs tend to refer to simpler technologies such as anonymization and pseudonymization, which focus on removing identifying data from datasets. Advanced PETs tend to refer to those that offer more robust privacy protections such as secure multi-party computation and homomorphic encryption. FPF (2024), "CPDP LatAm 2024: What is Top of Mind in Latin American Data Protection and Privacy? From data sovereignty, to PETs". Available at: https://fpf.org/blog/cpdp-latam-2024-what-is-top-of-mind-in-latin-american-data-protection-and-privacy-from-data-sovereignty-to-pets/

[60] Privacy Sandbox (n.d.), "How Mercado Libre is testing Privacy Sandbox to improve customer privacy". Available at: https://privacysandbox.google.com/resources/case-studies/mercado-libre

[61] Gov.br (2024), "Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados". Available at: https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados

healthcare, showcasing their potential to protect user data while enabling powerful analytics. Box 3 outlines examples of PET use cases across industries globally.

Box 3: Examples of PET use cases across various sectors

While the use of PETs in digital advertising remains relatively nascent, with limited large-scale deployments or published success stories, these technologies are not new and have already shown significant value in other sectors. Their applications in areas such as healthcare, finance, and the public sector demonstrate how PETs can enable secure data collaboration, regulatory compliance, and business innovation, focusing on user privacy. These examples serve to highlight the untapped potential for PETs in advertising and how they can support privacy-centric strategies. Some examples include:[62]

- **Homomorphic encryption in healthcare:** The United Kingdom's National Health Service (NHS), the country's group of publicly funded systems, has developed a system for securely linking patient data across different domains while maintaining confidentiality. Patient identifiers, such as NHS numbers, are pseudonymized through tokenization, with different tokenization schemes applied across domains for added security. Typically, linking data across domains would require removing tokenization, exposing personal information. To prevent this, the NHS employs a partially homomorphic encryption scheme, allowing datasets to be securely linked without revealing the underlying raw identifiers. This approach ensures that patient data remains protected while enabling critical healthcare analysis.

- **TEEs in tourism:** The Indonesian Ministry of Tourism leveraged mobile phone positioning data to better understand cross-border tourism activity. Since mobility data is highly sensitive, the analysis required collaboration between multiple mobile network operators while ensuring data privacy. Using Sharemind, a privacy technology from Cybernetica, the data was encrypted and processed within a TEE, preventing access to unencrypted data at any stage. The aggregated statistics, provided by Estonian data analytics firm Positium, now serve as a foundation for tourism statistics in Indonesia.

- **TEEs in finance:** The DANIE consortium, a financial data-sharing initiative, enables banks and data providers to securely analyze shared banking data for multiple purposes, including improving client data quality, detecting fraud, and preventing money laundering. Launched in 2020, DANIE uses encryption and TEEs provided by Secretarium, ensuring that no individuals have access to the processed data. This collaboration brings about improved compliance with EU reporting requirements, reduced costs for data review and remediation, and greater environmental efficiency in data management through centralized processing.

- **TEEs in digital advertising:** Google's Confidential Matching product uses TEEs to securely connect and leverage their first-party data for effective audience management. By processing data within isolated hardware environments, Google protects customer information from exposure while enabling accurate data analysis. This approach enhances privacy protections for advertisers and users alike, offering a robust framework for secure data collaboration without compromising utility.[63]

- **Multi-party computation in eldercare:** In the Netherlands, a public-private coalition including privacy tech company Linksight, health insurer DSW, and local health offices developed a data analysis platform using multi-party computation to securely analyze sensitive elderly care data. This

[62] Centre for Data Ethics and Innovation (n.d.), "Repository of Use Cases". Available at: https://cdeiuk.github.io/pets-adoption-guide/repository/
[63] Google Blog (2024), "Simpler data privacy for advertisers with confidential matching". Available at: https://blog.google/products/ads-commerce/google-confidential-matching-data-privacy/

platform aggregates data without exposing individual-level information, reducing privacy risks and overcoming data fragmentation across multiple parties. By enabling better insights into care needs, it supports more informed policymaking. Initially deployed in several regions, the initiative aims to scale nationally, demonstrating how PETs can facilitate secure, privacy-preserving data sharing for public benefit.[64]

3.2. Breaking down adoption barriers: the role of industry collaboration

Despite growing recognition of PETs as a promising tool for balancing data utility and privacy, their widespread adoption, particularly in the advertising sector—remains limited. Businesses face a range of challenges, from technical constraints and high implementation costs to uncertainty around compliance and a lack of cross-platform compatibility. In this context, industry collaboration emerges as a critical enabler for advancing PET uptake. Cross-sector partnerships, joint testing environments, and shared best practices can help lower the barriers to adoption, while coordinated efforts between regulators and the private sector can provide clearer guidance and build trust. Collaborative frameworks are essential not just for driving innovation, but for ensuring PETs can be applied at scale in a way that is technically feasible, economically viable, and legally sound.

3.2.1 Key roadblocks to PET adoption

Although PETs offer strong potential to support privacy-forward data practices, their adoption in digital advertising is still nascent and can be challenging to quantify. Businesses face a range of barriers such as cost, technical complexity and limited awareness, and the lack of real-world success metrics can make it more difficult to build a compelling business case around. Critically, what is often missing is clearer and more actionable guidance. Greater industry-led frameworks are essential to help organizations adopt PETs with confidence and at scale.

To better understand the state of PET adoption among businesses in the region as well as key roadblocks, Access Partnership conducted interviews with data protection and privacy executives in Latin America across March and April 2025 (Box 4). The conversations revealed that privacy concerns are becoming a strategic priority, with firms recognizing a need to rethink traditional advertising practices. Most professionals interviewed recognized specific technologies that they may already have implemented (for instance, differential privacy), but not all were familiar with the broader concept of PETs.

Adoption and awareness of PETs were also seen to be uneven across industries and business sizes. Many large enterprises, particularly those operating in multiple jurisdictions, are already investing in PETs to comply with regulatory requirements such as Brazil's LGPD. However, smaller businesses face significant barriers, including high costs, technical challenges, and a lack of clear regulatory guidance. Regulatory pressures and consumer expectations are pushing companies to act, but many remain reactive rather than proactive. Businesses recognize that PETs can enhance consumer trust and mitigate compliance risks, yet measuring their ROI remains a challenge. Without clear business-driven incentives, PET adoption tends to be deprioritized in favor of short-term commercial goals. Executives stress the need for stronger government support, industry collaboration, and standardized frameworks to facilitate wider adoption and ensure PETs are scalable and effective across the region.

[64] CoE-DSC (2023), "". Available at: https://coe-dsc.nl/use-cases/advancing-data-collaboration-for-monitoring-the-dutch-elderly-care-through-mpc-technology/

Box 4: Insights from interviews with data protection and privacy executives

Across March and April 2025, Access Partnership conducted interviews with data protection and privacy executives of leading organizations in Latin America, including data protection officers (DPOs), chief intelligence officers (CIOs), and data privacy directors. Interviewees spanned various industries such as e-commerce, healthcare, beauty, and advertising. These interviews were aimed at gathering insights on user perceptions of privacy issues as well as the adoption, challenges, and impact of PETs in the region.

Interview 1: Navigating privacy challenges in digital advertising

Ongoing signal loss and evolving privacy regulations are reshaping the digital advertising landscape, particularly across Latin America. As the industry grapples with increasing regulatory scrutiny, companies are exploring PETs to future-proof their operations. However, adoption remains complex due to platform interoperability issues and fragmented regulatory environments.

While client awareness of privacy risks is growing, many continue to prioritize short-term business outcomes over long-term data protection strategies. Measuring the return on investment for PETs remains a significant barrier, as privacy initiatives are often viewed as compliance costs rather than strategic assets. Furthermore, the value of PETs may only become visible in the medium to long term, making it harder to justify immediate investment.

Some companies are beginning to integrate privacy into their core operations, but achieving industry-wide alignment is still a challenge. Collaboration between advertisers, tech platforms, and regulators will be key to developing scalable privacy solutions that serve both compliance requirements and business goals.

Insights based on an interview with Caio Amorim, Data Protection Officer at WPP (Brazil), a global creative and marketing company.

Interview 2: Scaling privacy innovation in Mexico's evolving regulatory environment

As privacy concerns gain prominence in Mexico's digital ecosystem, businesses are beginning to invest in PETs to ensure compliance and strengthen consumer trust. However, adoption remains uneven. While larger companies are advancing quickly, small and medium enterprises face significant cost and technical hurdles that limit their ability to implement robust privacy solutions.

One of the key challenges is the inconsistency of regulatory enforcement. Although legal frameworks for data protection exist, varying interpretations and weak enforcement create uncertainty, making it difficult for companies to plan long-term investments in privacy infrastructure. Businesses also face technical challenges, such as interoperability issues and maintaining a seamless user experience while deploying PETs.

To drive more widespread adoption, clearer regulatory guidance and greater industry collaboration will be essential. While momentum is building, Mexico's privacy landscape will need stronger coordination to scale solutions that are both compliant and commercially viable.

Insights based on an interview with José Carlos Morales Alvarez, Former Chief Information Officer at Farmacia San Pablo (Mexico).

Interview 3: Balancing privacy compliance and business priorities in Latin American e-commerce

E-commerce platforms in Latin America are facing mounting pressure to comply with a growing patchwork of privacy regulations. While laws like Brazil's LGPD are helping set regional benchmarks, implementation remains complex across multiple jurisdictions. Companies are investing in PETs, but

challenges persist—from fragmented regulations to the difficulty of demonstrating clear business value.

Privacy remains a priority for leading platforms, but it is not yet a key business driver in the region. Consumer interest in privacy tends to surge only in response to major breaches, making it harder to sustain proactive investment. Internally, developing PETs—such as custom encryption tools—requires careful coordination across legal and technical teams. Yet without standardized KPIs, measuring the effectiveness and return on these investments is still a work in progress.

Key obstacles include prioritization of privacy in product development, a lack of regulatory clarity, and the ongoing need to align efforts across diverse markets. As privacy laws across Latin America evolve to emphasize accountability, collaboration within the industry will be essential to create scalable, standardized solutions.

Insights based on an interview with Pablo Segura, Regional Data Privacy Director, and Samanta Oliveira, DPO at Mercado Libre (Brazil), Latin America's largest e-commerce platform.

Interview 4: Embedding privacy in retail without compromising agility

As Brazil's retail sector undergoes rapid digital transformation, balancing privacy with operational agility is becoming increasingly complex. Unlike more heavily regulated industries, retailers face fewer compliance pressures, and privacy is not yet seen as a core business driver. This often results in privacy safeguards taking a backseat to the need for seamless, day-to-day operations—especially in large, decentralized organizations.

Companies are investing in security tools such as encryption, Data Loss Prevention (DLP) controls, and API credential management to reduce data exposure. Yet these tools are not always labeled or recognized internally as PETs, and awareness across business units remains moderate. Organizational scale, legacy systems, and ongoing integrations of newly acquired entities present additional hurdles to PET deployment.

Consumer demand for privacy in Brazil is also relatively muted compared to markets like Europe, where privacy has become a competitive differentiator. However, this is expected to change as AI-driven fraud and identity theft risks grow. To prepare, retail companies are recognizing the need for secure third-party data-sharing mechanisms and greater industry collaboration to standardize PET adoption and ensure resilience in the face of evolving threats.

Insights based on an interview with Isabella Becker (DPO), Luis Ribeiro, and Lais Litran (Privacy Specialists) at Grupo Boticário, one of Brazil's largest cosmetics retailers.

Broadly, there are four types of issues faced:

Interoperability challenges

While PETs hold promise for enhancing privacy, differing implementations across providers pose major barriers to seamless collaboration. For example, variations in secure multi-party computation protocols or differential privacy noise injection methods can make it difficult for businesses to adopt a plug-and-play approach. This is particularly challenging for advertisers and publishers who rely on cross-platform data sharing. The lack of cross-platform PET compatibility complicates integration and limits scalability, especially for companies operating across jurisdictions.

Cost considerations

Deploying PETs requires investment in both infrastructure and skilled personnel, which can be a barrier for smaller businesses.[65] Some PETs, like homomorphic encryption, demand significant computational resources, leading to higher operational costs due to limited scalability, increased processing time and cloud computing expenses.[66] Additionally, businesses must allocate budgets for training employees, hiring privacy engineers, and updating existing systems to accommodate PETs. While large technology firms may have the resources to absorb these costs, smaller advertisers and publishers may struggle to justify the financial investment without clear short-term returns. The lack of studies that conclusively highlight the positive ROI of PETs could also serve as a roadblock, as firms may find it difficult to obtain approval for implementation.

Limited education and awareness

Despite the growing focus on privacy, many advertisers and publishers lack a clear understanding of PETs and their potential benefits.[67] A lack of accessible resources and training programs means that many businesses remain unaware of how PETs can enable privacy-preserving advertising while maintaining ad effectiveness. Without greater awareness, decision-makers may perceive PETs as overly complex, leading to hesitation in adoption. Industry initiatives, such as workshops and training programs by organizations like the Future of Privacy Forum and IAB, can help bridge this knowledge gap and encourage more widespread implementation.

A principle-based approach

PETs are not a substitute for broad data protection laws such as regulations introduced by Brazil and Mexico. While they can support privacy goals, true compliance also depends on robust organizational policies and compliance with general privacy principles.

An Open Loop study conducted in Brazil highlighted that the LGPD primarily relies on these general principles instead of detailed, specific provisions for PETs.[68] This principle-based approach is designed to allow for the adoption of PETs without undue legal constraints, while providing a foundational framework. Nevertheless, providing more specific incentives, particularly concerning technologies like anonymization, would be a beneficial step. This would further encourage businesses developing PETs and facilitate clearer determination for data controllers and processors regarding how their privacy measures align with legal expectations.

3.2.2 The need for cross-industry collaboration to scale PET solutions

To address these challenges, cross-industry collaboration will be essential, necessitating action from stakeholders such as industry groups, advertisers, technology providers and regulators. Collaboration among these stakeholders can help improve PET interoperability with existing systems and lower implementation barriers through shared best practices and scalable solutions. Additionally, partnerships between regulators and industry players can ensure that privacy regulations align with technological advancements, facilitating smoother adoption while maintaining compliance.

Privacy advocacy groups also play a crucial role in shaping the privacy discourse, advocating for best practices, and engaging with both regulators and businesses on data protection matters. In the context of Latin America, organizations such as the Institute for Technology & Society of Rio de Janeiro (ITS Rio) and SaferNet contribute to the development of privacy frameworks, promote responsible data governance, and help bridge the gap between regulatory requirements and industry implementation. Their involvement can help foster a more privacy-conscious digital ecosystem while ensuring that PETs are developed and deployed in ways that align with user rights and expectations.

Both in Latin America and globally, several initiatives are already underway to accelerate the adoption of PETs more widely across various industries, including for digital advertising. For instance, in Singapore, the Info-Communications Media Development (IMDA) is facilitating experimentation with PETs through a Sandbox, which provides opportunities for companies to work with trusted digital solution providers to develop use cases and pilot PETs.[69] The Sandbox will matchmake use case owners to PET providers, provide grant support to companies for the scoping and implementation of

[65] CIPL (2023), *Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age*. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf

[66] Super Micro (n.d.), "What Is Homomorphic Encryption?". Available at: https://www.supermicro.com/en/glossary/homomorphic-encryption

[67] Future of Privacy Forum (2025), *Privacy Enhancing Technologies: A State Education Agency Landscape Analysis.* Available at: https://fpf.org/wp-content/uploads/2025/03/Privacy-Enhancing-Technologies-An-Education-Landscape-Analysis.docx.pdf

[68] Open Loop (2024), "Prototyping Privacy-Enhancing Technologies Guidance in Brazil". Available at: https://openloop.org/reports/2024/04/brazil-report-pets-en.pdf

[69] IMDA (2024), "Privacy Enhancing Technology Sandboxes". Available at: https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes

pilot projects, and provide regulatory support to ensure compliant deployment of PETs. One successful implementation example from this pilot is Mastercard, a global technology company, that has since developed a proof of concept (POC) in the Sandbox to investigate a product based on fully homomorphic encryption provided by a third party.[70] This has facilitated the sharing of financial crime intelligence across international borders while complying with prevailing regulations.[71]

While PETs represent a significant step forward in protecting consumer privacy while enabling data-driven innovation, they are not a silver bullet. Their effectiveness depends on a broader ecosystem of enablers, including education, awareness, and general and broad data protection principles. Businesses and consumers benefit from greater awareness of how PETs function and the solutions they offer to build trust and encourage widespread adoption. Capacity-building initiatives, such as training programs for businesses and consumer education campaigns, can further reinforce responsible data practices.

At the same time, it is important to recognize the risks of PET misuse or over-reliance. Without appropriate boundaries, PETs could create a false sense of compliance or obscure harmful practices, such as concealing the true scope of unauthorized data collection by obscuring the underlying data flows and linkages. To fully realize the benefits of PETs, stakeholders must combine their use with strong accountability measures, such as general privacy principles and ethical standards. By combining PETs with these measures, stakeholders can create a more privacy-preserving digital ecosystem that fosters both innovation and consumer trust.

[70] IMDA (n.d.) "Preventing financial fraud across different jurisdictions with secure data collaborations". Available at: https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--mastercard.pdf

[71] IMDA (n.d.) "Preventing financial fraud across different jurisdictions with secure data collaborations". Available at: https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--mastercard.pdf

4. Conclusion

The shift toward a privacy-forward digital ecosystem is no longer optional, it is an imperative for businesses seeking to remain competitive. PETs provide a vital pathway for advertisers and technology providers to achieve data protection and a robust and effective digital advertising ecosystem.

With the decline of traditional tracking methods and increasing scrutiny of data practices, advertisers must adapt to meet the moment. PETs offer a way to continue delivering relevant, personalized advertising while respecting user privacy. By employing techniques such as differential privacy, federated learning, and secure multi-party computation, advertisers can analyze user data and measure campaign effectiveness in a privacy-preserving manner. Businesses that proactively integrate PETs into their advertising strategies will be better positioned to maintain consumer engagement and trust in an era of heightened privacy awareness.

However, despite their potential, PETs remain underutilized due to challenges such as technical complexity, and high implementation costs. Overcoming these barriers requires a coordinated effort from industry groups, advertisers, technology providers, civil society, and regulators. Cross-industry initiatives and collaborative frameworks between the public and private sectors play a crucial role in advancing PET innovation and adoption. Rather than pushing for uniform standards, these efforts should focus on providing clearer guidance, practical implementation pathways, and shared resources. Such collaboration

can increase PET adoption, making privacy-centric advertising solutions more accessible, interoperable, and scalable.

The transition to a privacy-forward digital ecosystem is inevitable, and PETs could be at the core of this evolution. Businesses that invest in PETs today will not only enhance consumer trust but also futureproof their operations. By embracing PETs, advertisers and industry leaders can build a sustainable digital economy that respects user privacy while ensuring that advertising remains an effective and viable tool for growth. Through collaboration, innovation, and proactive adoption of PETs, Latin America's digital ecosystem can set a global standard for privacy-forward advertising. Key takeaways and top actions to accelerate adoption are summarized in Box 5 below.

Box 5: Key takeaways and top actions to accelerate PET adoption

While PETs enable data to be analyzed or shared in ways that aim to protect user privacy, several technical and operational limitations still hinder their broader adoption and effectiveness:

Key takeaways:

- PETs enable the balance between effective advertising and stronger consumer privacy protections
- Consumer trust and regulatory pressure are accelerating the shift toward privacy-centric solutions
- PETs are essential but must be supported by education, governance, and industry collaboration
- Adoption of PETs will give businesses a competitive advantage in a changing regulatory and market environment

Top actions to incentivize and accelerate PET adoption:

- Data Protection Agencies:
  - Provide incentives for anonymization and data minimization techniques
  - Encourage innovation through sandboxes, pilot projects, and research funding
- Industry Stakeholders:
  - Collaborate on the development of frameworks to facilitate interoperability, and encourage standardization on a consistent high bar for the use of specific types of PETs
  - Develop and share best practices, and make data and test environments available, to lower development and implementation barriers
- Advertisers and technology providers:
  - Invest in capacity-building initiatives, including technical training and consumer education, to drive trust and understanding
  - Integrate PETs proactively into advertising strategies, rather than waiting for regulatory mandates

Access Partnership

accesspartnership.com

Follow us

Our offices

Europe

London

The Tower, Buckingham Green
Buckingham Gate
London, SW1E 6AS
United Kingdom

+44 20 3143 4900
london@accesspartnership.com

Brussels

8th Floor, Silversquare Europe
Square de Meeûs 35
B-1000 Brussels
Belgium

brussels@accesspartnership.com

North America

Washington DC

1300 Connecticut Avenue NW,
Suite 250
Washington, DC 20036
USA

+1 202 503 1570
washingtondc@accesspartnership.com

Asia

Singapore

Asia Square, Tower 2
#11-2012
Marina View
Singapore 018961

+65 8323 7855
singapore@accesspartnership.com

Jakarta

Revenue Tower 21st Floor
Unit 104 SCBD Lot 13, Jl. Jend. Sudirman
Kav. 52-53
Provinsi DKI Jakarta, 12190
Jakarta, Indonesia

+62 21 5020 0949

Kuala Lumpur

Common Ground Q Sentral
Level 39, Unit 39-02 (East Wing),
2A,
Jalan Stesen Sentral 2, Kuala
Lumpur Sentral, 50470
Kuala Lumpur, Malaysia

Bangkok

188 Spring Tower
11th Floor, Unit 106, Phayathai
Road
Thung Phayathai, Ratchathewi,
10400Bangkok, Thailand

+ 66 (2)-8216148

Hanoi

19th floor, Tower 1
Capital Place Building
No 29 Lieu Giai Street
Ngoc Khanh Ward, Ba Dinh Diítrict
Hanoi, Vietnam

Manila

28F & Penthouse
World Plaza
5th Ave
Bonifacio Global City
Manila, 1634
Philippines

Middle East and Africa

Abu Dhabi

Al Wahda City Tower, 20th Floor
Hazaa Bin Zayed The First Street
PO Box 127432
Abu Dhabi, UAE

abudhabi@accesspartnership.com

Johannesburg

119 Witch-Hazel Avenue
Highveld Technopark
Johannesburg
Gauteng, South Africa