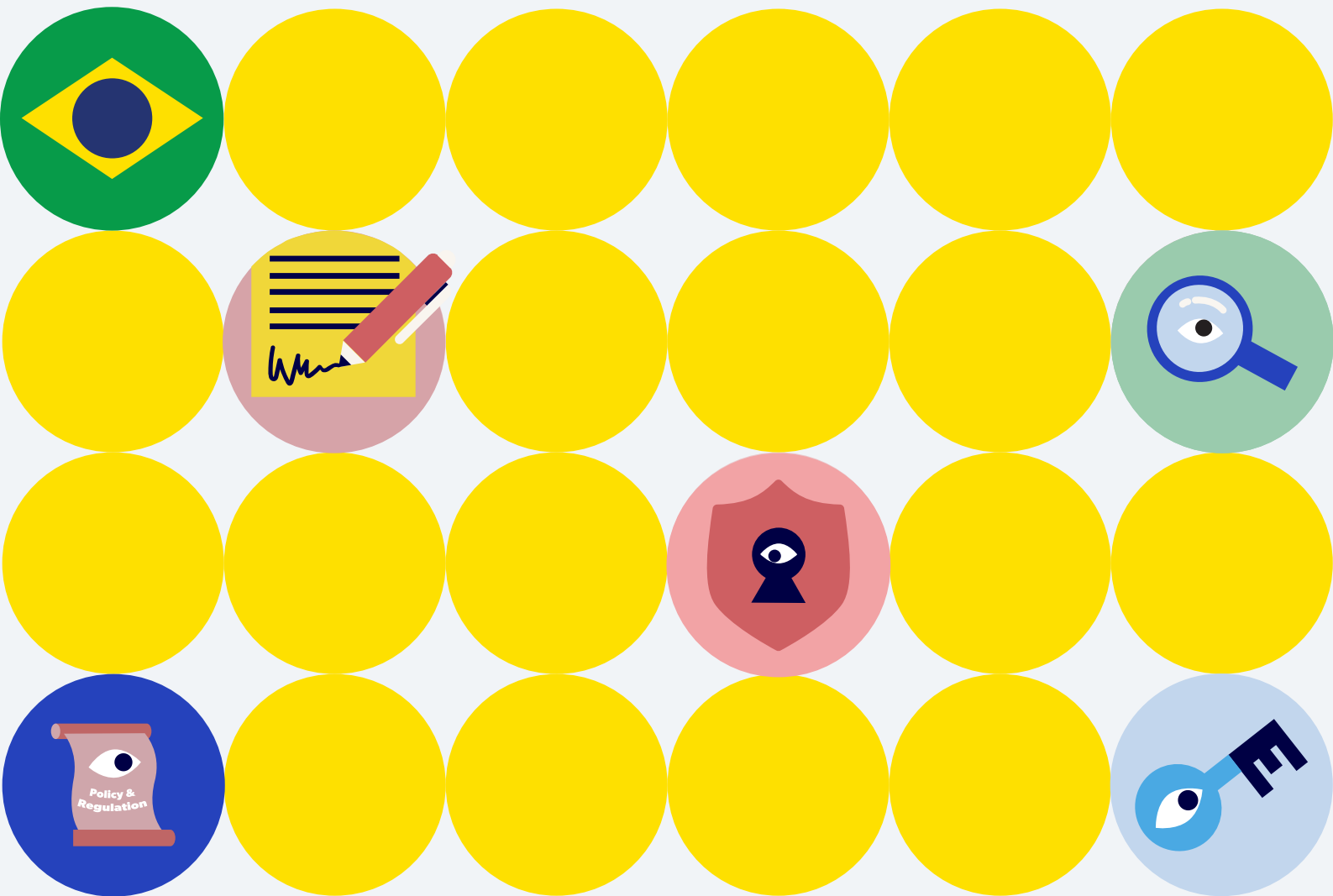


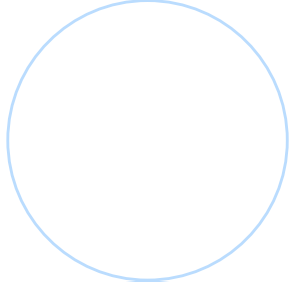
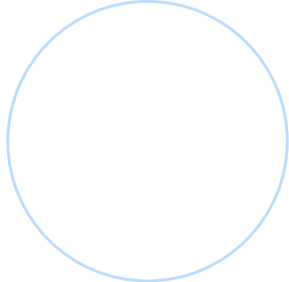
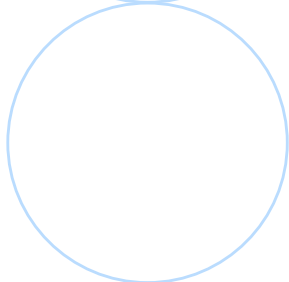
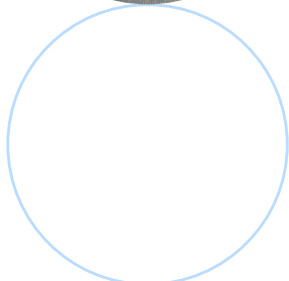
Prototyping Privacy-Enhancing Technologies Guidance in Brazil



Index

→	Executive Summary	8
1	Introduction	10
	What are PETs?	12
	Global policy landscape	13
	About the policy prototype	15
	About the testing	16
2	About the Open Loop Brazil Program	17
	Local policy landscape	18
	About the cohort	19
3	Findings	20
	3.1 Companies reported a low familiarity with PETs, especially advanced ones	21
	3.2 The PETs playbook helped companies to identify privacy risks and mitigation strategies	21
	3.3 Companies experienced a burden of costs and human resource constraints.	22
	3.4 Regulatory uncertainty is a key barrier to PET adoption	23
4	Policy Recommendations	24
	4.1 Regulatory certainty and incentives for PETs adoption	25
	4.2 Multi-stakeholder dialogues around best practices and standards	26
	4.3 Direct investment in research, development, and education	27
	Conclusion and next steps	28
	Annex 1 - Methodology	29
	References	30

Foreword



Meta's Open Loop programs in Brazil and Uruguay, conducted between 2022 and 2023, mark a significant milestone in the advancement of policy prototyping tools and methodologies for governing emerging technologies in Latin America, in a context in which the notion of policy experimentation and regulatory sandboxes seem to have become an integral part of policymaking in the public and the private sectors.

After a successful program on transparency and explainability in Mexico, Open Loop turned to the South Cone to run a parallel experiment on Privacy-Enhancing Technologies (PETs) in partnership with independent implementation teams and several participating companies in Brazil and Uruguay. This effort provided a great opportunity to dive deep into each country's peculiarities, their policy and institutional ecosystems, and the nature of the players starting their PETs adoption journey in each jurisdiction. It also offered a singular opportunity to understand how valued PETs are for the protection of personal data across the board, and to map out similarities that exist in both contexts in terms of challenges and opportunities around the wider adoption and use of PETs.

In a nutshell, Open Loop Brazil and Uruguay generated three important outcomes: first, the programs contributed to raising awareness and to developing capacity on the topic of PETs during the early stages of the program; second, by leveraging a consortium of companies, experts and policymakers, the program sparked multi-stakeholder dialogues and knowledge sharing in both countries (including across borders) that are likely to endure even after the conclusion of that journey; and, finally, the collective and collaborative effort produced sound and reliable evidence that will most certainly feedback into policy-making processes across the region and beyond.

As we express our gratitude to all the participant companies, observers, researchers and Meta colleagues who helped us build and develop Open Loop Brazil and Uruguay, we seize this opportunity to express our confidence that this final report represents an important and decisive first step in connecting tech and policy innovation, fostering a closer collaboration between those building emerging technologies and those regulating them in Latin America.

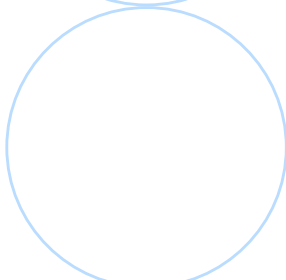
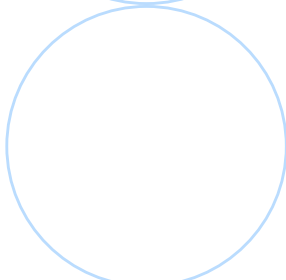
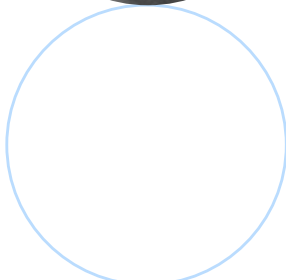
Paula Vargas

Director, Privacy Policy & Engagement, Latam

Diego Rafael Canabarro

Head of Privacy Policy, Latam

Foreword



In April 2024, Privacy-Enhancing Technologies (PETs) were ranked number two among the World Economic Forum's "Top 10 Emerging Technologies to Address Global Challenges." This recognition underscores the critical importance of safeguarding privacy in an era of rapid digital transformation and the swift evolution of data-driven technologies, including Artificial Intelligence (AI). As the digital landscape continues to expand, it presents both challenges and opportunities for innovative solutions that balance data utilization with personal privacy.

As civil society organizations operating within the technological sphere, both the Instituto Liberdade Digital and C Minds' Eon Resilience Lab (a Mexican organization exploring the intersection between emerging tech, social, and environmental impact) are committed to developing strategies that minimize the potential risks of emerging technologies while maximizing their positive social impact. By experimenting with these topics, we can draft human-centered policy recommendations based on our learnings and aligned with global practices and standards.

Given the significant opportunities PETs represent, it is crucial to further explore and understand how Latin American markets can continue to leverage data-processing tools while protecting individual privacy. The Open Loop program provided an exciting opportunity not only because such exercises serve as dynamic mechanisms to bridge the gap between theoretical discussions and tangible solutions, but also they bring diverse perspectives as they involve a diverse range of stakeholders, including government, academia, industry, and civil society. These collaborative endeavors facilitate a holistic comprehension of the subtleties of PETs in specific context, ensuring that our findings would translate into comprehensive and sustainable recommendations.

In a global context where PETs are being prioritized, the publication of our findings positions Latin America at the forefront of international conversations. This strengthens the region's ability to contribute unique perspectives and innovations to the global dialogue on technology and data protection. These insights are a crucial step towards ensuring that the benefits of digital transformation are realized broadly and fairly, reinforcing the region's role as a leader in the global technology landscape.

This report is not only a reflection of our commitment to responsible technology deployment but also a vital resource for people striving to navigate the complexities of AI and data privacy. We hope that the findings in this report will contribute to expanding society's knowledge concerning PETs, help entities and governments in the process of implementing these technologies, to foster inclusive and collaborative spaces and discussions and support policymakers in the drafting of further privacy-related frameworks.

Constanza Gómez-Mont
President and Founder at C Minds

Maria Marinho
Co-fundadora do Instituto
Liberdade Digital

Cláudio Lucena
Universidade Estadual da Paraíba

Foreword



In an era defined by the rapid evolution of technology, with a growing emphasis on artificial intelligence (AI), the challenge of efficiently managing questions relating to privacy is gaining more and more prominence. AI systems process large quantities of personal data, so the need to protect privacy through robust tools has never been too critical. In this context, privacy protection technologies (PETs) emerge as crucial tools, offering mechanisms to balance innovation with individual rights and societal trust.

As PETs help promote transparency and trust in AI systems, empowering individuals with greater control over their data and, at the same time, promoting safe collaborations for the establishment of effective data governance. In this way, these technologies also help to promote an ethical AI ecosystem, where innovation can flourish without compromising fundamental rights.

The Open Loop program explores the positive potential in the formulation of public policies that promote PETs, including as regulatory compliance mechanisms. In addition to the ability to address the challenges inherent to two 'traditional' models of human data governance, PETs can also facilitate the evolution of new scenarios regarding AI management and governance systems.

It is important to highlight the inclusive format as the program was structured and implemented. Researchers, participants and observers have the opportunity to contribute to a broader understanding of the role of PETs, such as case studies and discussions on public policy prototyping.

The adoption of innovative, safe and predictable technologies has the potential to help provide legal security in the management of data in AI solutions, precisely at a time when several countries are discussing possible alternatives and regulatory formats, with expectations of compliance and never always clear. In fact, the work conducted does not program the topic of its amplified relevance also in the comparative scope between more than one country (also two various points of comparison with European regulations), or that generates reflection on how PETs can help to harmonize the confrontation of privacy management in different systems.

The report presents data and evidence in an accessible manner, without compromising the technical rigor of the methodology, with actionable conclusions that allow the creation of a concrete agenda in relation to technology.

Parabenizo or time of the program for plural mobilization and result of work, with the certainty that this report will contribute to constructive discussions in the formulation of public policies, both in the specific field of privacy, as well as in a broader way in relation to AI.

Eduardo Paranhos

Co-Leader of the Artificial Intelligence Working Group of the Brazilian Association of Software Companies (ABES). Partner at EPG Advogados

About the program and this report

Meta’s Open Loop is a global program that connects policymakers and technology companies to help develop effective and evidence-based policies for AI and other emerging technologies.

Through a structured methodology, Open Loop participants co-create policy “prototypes” and test new or existing AI policies, regulations, laws, or voluntary frameworks. These multi-stakeholder efforts support rulemaking processes and improve the quality of guidance and regulations on emerging technologies, ensuring that they are understandable, effective and feasible in practice.

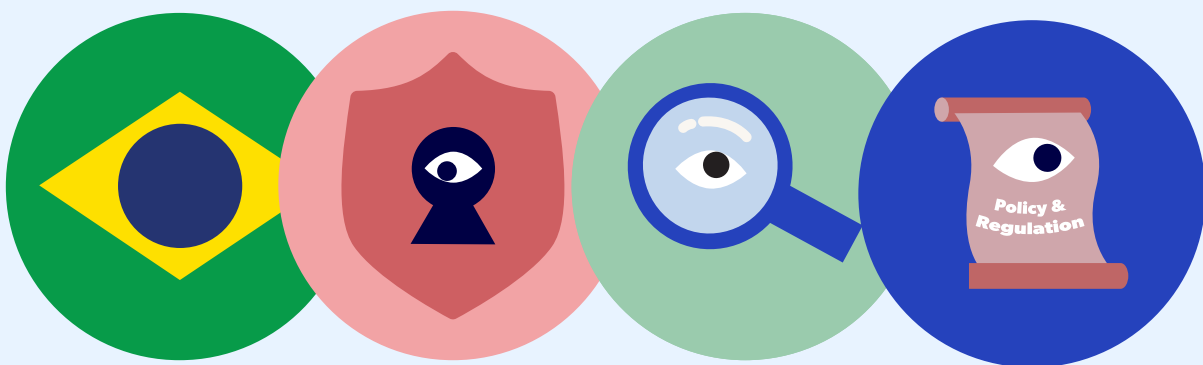
This report presents the findings and recommendations of the Open Loop Brazil program on PETs, launched in September 2022. This policy prototyping program began simultaneously with an identical program in Uruguay, with the intention of guiding and enabling companies in both countries to leverage and apply PETs to help reduce the identifiability of data and mitigate privacy-related risks, including in AI systems. Both programs were developed independently, and each had its own local partner responsible for implementing the program. The Open Loop Brazil program was rolled out in Brazil from September 2022 to April 2023 in partnership with Instituto Liberdade Digital.

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Written by: This report was written by Maria Marinho, Cláudio Lucena, David Lehr, Laura Galindo, Maartje Nugteren, and Diego Rafael Canabarro.

How to cite this report?

Marinho, Maria; Lucena, Cláudio; Lehr, David; Galindo, Laura; Nugteren, Maartje; and Canabarro, Diego Rafael. "Prototyping Privacy-Enhancing Technologies Guidance in Brazil" (2024), available at https://openloop.org/reports/2024/04/Brazil_Report_PETs_en.pdf



Acknowledgements

The Open Loop Brazil program was created by Meta and co-designed and facilitated in collaboration with Instituto Liberdade Digital.

We would like to thank the below Observer Organizations for participating in this initiative:



The Open Loop Program acknowledges the individual experts that represented the observer organizations throughout the program: Clara Langevin (C4IR), Eduardo Paranhos (EEBIA Axis I, Co-Leader of the ABES AI WG), Loren Spíndola (EBIA Axis I, Co-Leader of the ABES AI WG), Loren Spíndola (EBIA), Marcelo Guedes (ANPD), and Thiago Moraes (ANPD).

We would like to express our gratitude and recognition to the companies that collaborated in the development of this project:



A special thank you to the individual experts that represented the participating companies throughout the program: Caroline Rocabado (Dasa), Charles Buss (Beetools), Cinthia Baccarin (Mercado Livre), Diego Pereira (Peakinvest), Expedito Junior (Antares Comunicação), Jefferson Araújo (Showkase), Kleber Santos (Vectras), Matheus Crispim (Neoron), Miguel Isoni Filho (Neoron), Raíssa Moura (Nubank), Nathália Sampaio (Dasa), Rawlisson Terrabuio (Beetools) Samantha Santos de Oliveira (Mercado Livre) e Thaís Souza (Peakinvest).

Thank you in particular to our group of experts, who shared their deep expertise and contributed to the development of the program's research strategy: Ana Paula Bialer, Ângela Rosso, Carlos Affonso de Souza, Diogo Cortiz, Gustavo Godinho, Maria Cecília Oliveira Gomes, Núria Lopez, Raquel Saraiva, Savyo Moraes, Tatiana Coutinho e Wellington Dantas.

Thank you also to our design partners at Craig Walker Design and Research, in particular John-Henry Pajak.

Executive Summary

Open Loop is a global program that connects policymakers and innovative companies to help develop effective and evidence-based policies around AI and other emerging technologies. The primary objective of this Open Loop program was to guide and enable companies in both Brazil and Uruguay to leverage and select PETs to help reduce the identifiability of data and mitigate privacy-related risks, including in AI systems.

To bridge the gap between privacy expectations and technology solutions and empower data controllers to process data in a privacy-centric manner, a policy prototype was developed and tested in the shape of a technical playbook for advancing data protection principles using PETs. This policy prototype aims to support companies by setting out data protection principles and guiding them through a 3-step process for operationalizing privacy by design principles while connecting them to the adoption of PETs.

This report shares the results of this policy prototyping program, which was rolled out in Brazil from September 2022 to April 2023 in partnership with Instituto Liberdade Digital and involved 9 companies from Brazil. These companies all provide B2B and/or B2C services and are of varying sizes and sectors.

The program investigated:

- How effectively the policy prototype balances policy clarity, technical feasibility, and policy effectiveness for its intended audience.
- Participating companies' current familiarity and understanding of PETs.
- Current gaps and implementation challenges for PETs adoption by organizations in Brazil and Uruguay.
- Best practices and learnings that contribute to the successful adoption of PETs to help reduce the identifiability of data and mitigate privacy-related risks.

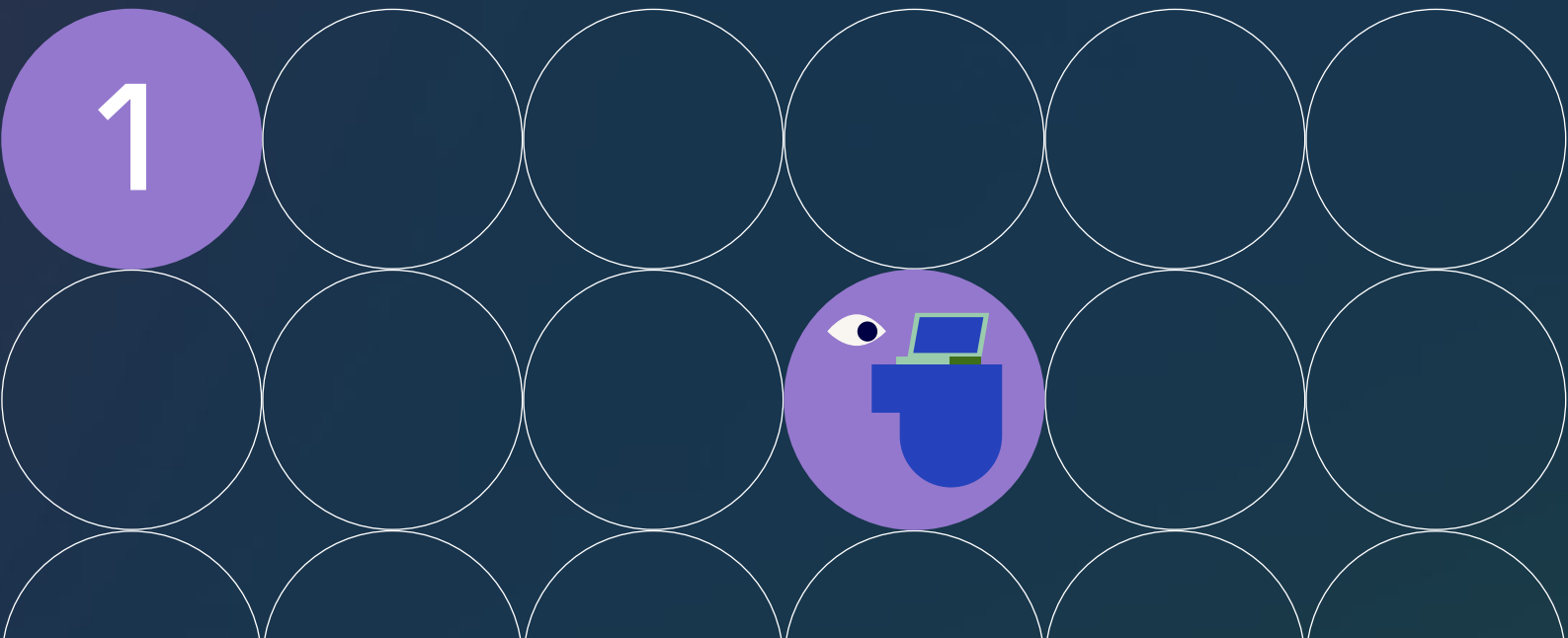
Our findings demonstrate that in both Brazil and Uruguay:

- Companies reported a low familiarity with PETs, especially advanced ones.
- The PETs playbook helped companies to identify privacy risks and mitigation strategies.
- Companies experienced a burden of costs and human resource constraints.
- Regulatory uncertainty is a key barrier to PET adoption.

Based on the results of the Open Loop Brazil and Uruguay programs and the feedback received from participating companies, the following recommendations are offered to regulators and policymakers responsible for data governance, privacy, and data protection concerning PETs:

- 1 Policymakers should embrace a flexible, risk-based approach to the legal concept of anonymization:** Measuring the level of risk should be a fact-specific assessment that considers the context of data processing, what technical measures (such as PETs) have been applied to the data, and what non-technical measures (such as access controls and legal restrictions) have been applied to the data. Also, measuring risk should focus on whether parties who might realistically get access to the data could re-identify the data given all of the protections that have been applied to it.
- 2 Policymakers should clarify that entities can process data for the purpose of reducing the risk of identifiability:** In particular, for jurisdictions that rely on GDPR-like laws—those under which a legal basis is required to process data—policymakers should clarify either that: (i) no legal basis is needed for processing data for the purpose of reducing the risk of identifiability; or (ii) legitimate interests, or a similar legal basis, can readily be relied upon to conduct such processing.
- 3 Policymakers have a valuable role to play in advancing multi-stakeholder dialogues around PETs:** Not only could these conversations help to build entities' capacities to deploy PETs, but they could also make progress on developing a shared understanding of PETs and how they can be effectively used in different use cases. Policymakers could convene dialogues to explore these intricacies, seeking participation from standards-setting bodies and industry-wide associations in the process.
- 4 Policymakers should directly invest in PETs research and development, as well as public education about the benefits of PETs:** Policymakers could also fund R&D into open-source PETs implementations, which could be more readily used off-the-shelf by small and medium entities. In addition to R&D, policymakers could invest in public education campaigns that help explain to individuals how PETs can protect their privacy.
- 5 Additional considerations:** Policymakers are encouraged to explore the above topics more thoroughly through regulatory sandboxes.

Introduction



As technologies that analyze large amounts of data have advanced, so have technologies that create new opportunities for augmenting individuals' privacy. **Privacy-enhancing technologies** (“PETs”) hold significant potential to address many privacy risks while still enabling the society-wide benefits that come with cutting-edge data analysis.

The recognition of these benefits has led to a spike in interest in PETs—from industry, policymakers, and privacy advocates alike—over the last few years. But, as more vigorous discussions around PETs develop, it becomes critical for all stakeholders to have deeper understandings of PETs, the practicalities of using them, and the ways in which public policy can incentivize or disincentivize their use.

Meta's Open Loop program sought to foster these understandings through related initiatives in Brazil and Uruguay, bringing together local experts, companies, and observers in each country. These initiatives aimed to develop companies' capacities to deploy PETs and, in the process, interrogate the challenges that emerged and how policymakers can address these challenges.

This report presents the key findings and policy recommendations from the initiatives in Brazil and Uruguay. The rest of this introductory chapter provides a brief introduction to PETs, summarizes the global policy landscape related to PETs and describes the common methodology of the initiatives in Brazil and Uruguay. The second chapter focuses on unique aspects of the initiative in Brazil, including its participants and the local policy landscape. Chapter three synthesizes the experiences in Brazil and Uruguay to draw out a set of key findings. Finally, the last chapter leverages these results to make recommendations for how policymakers can advance PETs adoption.

What are PETs?

PETs are an extremely diverse set of technical tools that operate in very different ways. At a high level, PETs are cryptographic or statistical techniques that preserve the informational value of data while enhancing privacy or security. But within this broad definition are many different techniques. **There is no one correct way to categorize PETs, but one potential way is to group them into four types:**



Data-altering PETs: Those, such as pseudonymization or differential privacy, that change the underlying data in some way;



Computation-altering PETs: Those, such as secure multiparty computation or federated analytics, that change who computes a function on data or how they do so;



Data-shielding PETs: Those, such as homomorphic encryption, that encrypt data or the media on which it is stored; and



Privacy-preserving machine learning: Techniques, such as synthetic data or adversarial attacks, that can be used to enhance and/or assess privacy protections in machine learning/AI (and often in other contexts too).





Another potential categorization of PETs comes from the OECD², which groups PETs into four different categories: data obfuscation tools, encrypted data processing tools, federated and distributed analytics, and data accountability tools. Again, there is no right way to categorize PETs, but groupings like these can provide heuristic value.









Regardless of how PETs are categorized, there are additional nuances that make talking about and deploying PETs difficult. First, PETs vary greatly in terms of maturity. Some PETs, such as standard encryption protocols, have existed for decades, whereas others, such as homomorphic encryption and federated learning, are much newer and are still being researched. Second, because PETs operate in different ways, they provide different kinds of privacy protections, some of which are easier to understand than others. For example, it is relatively easy to understand how removing a direct identifier like someone's name from a dataset preserves their privacy, but other techniques, such as secure multiparty computation, enhance privacy in more indirect, less intuitive ways. Finally, although PETs can be deployed in isolation, in practice they are often combined not only with other PETs, but also with non-technical privacy-enhancing tools, such as access controls and contractual restrictions on data use. Technical and policy conversations around PETs must recognize and embrace these complexities.

Global policy landscape

As PETs have advanced, so has global interest in them. Governments and international institutions are increasingly expressing optimism about the role that PETs can play in improving privacy, and they are eager to further investments in PETs in their jurisdictions. Table 1, below, presents a non-exhaustive snapshot of ways in which policymakers are attempting to meet these goals. Importantly, Table 1 does not include examples from Brazil or Uruguay; efforts in Brazil will be described in Chapter 2.

Table 1. A sampling of PETs-oriented initiatives and policies.

Region/Institution	Initiative/Policy	Description
United States 	National Strategy to Advance Privacy-Preserving Data Sharing and Analytics ³	The White House Office of Science and Technology Policy established this strategy to advance the use of techniques like PETs. Among other things, it encourages federal agency adoption of PETs, increased investments in research and development, increased education about PETs, and great international collaboration on the topic.
United States 	Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence ⁴	To enhance privacy in AI, the Order directs the formation of a Research Coordination Network on PETs, as well as the identification by federal agencies of opportunities for using PETs.
United States 	National Institute of Standards and Technology (NIST) Guidelines for Evaluating Differential Privacy Guarantees ⁵	This bill would direct NIST to fund research into PETs, and would direct federal agencies to collaborate on policy mechanisms for advancing PETs adoption, including the voluntary standards and guidelines.
United States 	Privacy Enhancing Technology Research Act ⁶	This bill would direct NIST to fund research into PETs, and would direct federal agencies to collaborate on policy mechanisms for advancing PETs adoption, including the voluntary standards and guidelines.

<p>United Kingdom</p> 	<p>Information Commissioner’s Office (ICO) <u>draft guidance</u> on anonymization, pseudonymization, and PETs, and final guidance on PET⁷</p>	<p>The ICO consulted on detailed, 5-part draft guidance, including a chapter on anonymization, and then published a more limited-in-scope final PETs guidance, referencing the draft guidance for additional details.</p>
<p>United Kingdom & United States</p> 	<p>PETs prize challenges⁸</p>	<p>The US and UK governments partnered to fund the development of PETs solutions for particular use cases.</p>
<p>European Union</p> 	<p>European Data Protection Board (EDPB) guidance revision</p>	<p>The EDPB indicated in its 2023-24 work program⁹ an intent to revise its anonymization guidelines.</p>
<p>European Union</p> 	<p>European Union (EU) General Court <u>decision</u> in SRB vs. EDPS¹⁰</p>	<p>This court decision emphasized that context matters for determining whether data have been anonymized under GDPR, and that, when data is shared, one must put oneself in the shoes of the recipient to assess re-identification risk.</p>
<p>Singapore</p> 	<p>Personal Data Protection Commission Singapore (PDPC) and Infocomm Media Development Authority (IMDA) regulatory sandbox¹¹</p>	<p>This regulatory sandbox evaluated case studies from companies, including Meta¹², answering companies’ questions about the application of data protection laws.</p>
<p>South Korea</p> 	<p><u>Revised guidelines</u> for pseudonymous data¹³</p>	<p>These revised guidelines addressed the processing of pseudonymous data, particularly in the context of AI.</p>
<p>International</p> 	<p>OECD PETs report and workshops¹⁴</p>	<p>OECD’s comprehensive report on PETs will be followed by workshops exploring use cases and policy issues.</p>
<p>International</p> 	<p>UN PETs task team¹⁵</p>	<p>The task team is focused on enhancing the use of PETs in countries’ national statistics offices.</p>

Although Table 1 presents merely a snapshot of PETs-related efforts around the world, the diversity of efforts makes clear that PETs is an increasingly important topic for stakeholders. In particular, governments have expressed significant interest in driving the adoption of PETs, both within the public sector and in broader society and industry. Another takeaway is that the exact relationship between PETs and data protection laws is uncertain and a subject of active exploration by regulators and courts. Most data protection laws do not deal with PETs directly; that is, they do not contain provisions specifically referencing PETs. That said, most data protection laws have fundamental principles—such as privacy by design, data minimization, and security—that PETs may serve to advance. Also, most laws exempt from their scopes data that has been “anonymized,” “de-identified,” or “dissociated.”¹ PETs may achieve this, but jurisdictions are grappling with exactly what the bar for this type of data transformation is. Jurisdictions like the UK and Singapore are embracing a flexible, risk-based approach, and the EU General Court’s decision in SRB seems to be pushing EU law in this direction as well. But significant uncertainties (including an appeal of the SRB decision) remain.

About the policy prototype

Meta’s Open Loop developed the **PETs Playbook (the “Playbook”)** to serve as the program’s policy prototype. The Playbook is an educational document that sought to help program participants understand more about PETs, how they can reduce privacy risks, and how they can be implemented. To accomplish these goals, the Playbook set out a three-step process, asking participants to do the following:

STEP 1

Risk Assessment

Participants were reminded of principles that guide data protection, and were asked to map their data lifecycles and assess potential privacy risks by taking into account both the likelihood of unintended or unexpected data processing and the magnitude of harms that could result from such processing.

STEP 2

Identify Risk-Reducing Strategies

With potential risks identified, participants were then asked to identify which strategies they could employ to reduce these risks. Potential strategies included data-oriented ones (minimization, separation, aggregation, and hiding) and organization- or process-oriented ones (informing, controlling, demonstrating, and enforcing).

STEP 3

Select Relevant PETs

Finally, the Playbook asked participants to select and evaluate the application of PETs that were responsive to the risk-reducing strategies they identified in Step 2. The PETs available for selection included de-identification techniques, differential privacy, synthetic data, federated learning/analytics, trusted execution environments, secure multiparty computation, encryption techniques, and homomorphic encryption.

About the testing

This Open Loop program employed a mixed methods approach to answering key questions surrounding their experiences with the Playbook (Annex 1 for more details). The findings presented in this report were identified through online survey responses, sequential and thematic workshops, and semi-structured interviews with participating companies.

In particular, the testing phase sought feedback—for each step of the Playbook—on three important aspects of the step:



Clarity

How clearly communicated and understandable the step was.



Effectiveness

How well the step achieved its goal (e.g., how well Step 3 enabled companies to identify the appropriate PETs).



Feasibility

How readily, given operational and real-world constraints, the participants could act on the prescriptions in a step.

The Program in Brazil

The Open Loop program in Brazil was conducted with Instituto Liberdade Digital as the local partner responsible for implementing the program. This section provides more detail on why and how the program in Brazil was conducted, including how the policy environment in Brazil was ripe for an exploration of these topics, and which Brazilian entities participated in the program. Those details for the Open Loop program in Uruguay can be found in [the Uruguay report](#)



Local policy landscape

As described in Chapter 1, one challenge of policy conversations surrounding PETs is the unclear link between PETs and data protection laws. Most comprehensive data privacy laws do not contain provisions explicitly mentioning PETs or how they could or should be used. Instead, such laws contain general data protection principles, such as data minimization, which PETs may help to achieve, as well as exemptions of anonymized data, which PETs may help to create.

Brazil's Lei Geral de Proteção de Dados Pessoais ("LGPD") follows this general approach. Article 12 exempts from the scope of personal data "anonymized data," and Article 5 defines "anonymized data" as "data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing." These provisions are similar in some ways to the relevant provisions of GDPR, whose Recital 26 treats as anonymous "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." Recital 26 also states, "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used . . . either by the controller or by another person to identify the natural person directly or indirectly."

But there are a few notable textual differences between LGPD and GDPR. First, they seem to differ with respect to which actors are considered when assessing the risk of identifiability. LGPD seems to focus on assessing whether the data controller or processor possesses means reasonably likely to be used to re-identify data. Article 12, Section 1, states that "the determination of what is considered reasonable shall take objective factors into account, such as cost and time necessary to reverse the process of anonymization, depending on the available technology, and the exclusive use of its own means" (emphasis added). GDPR, on the other hand, looks to means reasonably likely to be used "either by the controller or by another person" (emphasis added).

Second, LGPD and GDPR seem to differ based on whether reasonably available means are those available at the time of processing or also potentially in the future. LGPD's definition of "anonymized data" looks to technical means available "at the time of the processing," whereas GDPR's Recital 26 requires a consideration of "the available technology at the time of the processing and technological developments" (emphasis added).

The importance of these textual differences is unclear. As alluded to in Chapter 1, there is significant uncertainty surrounding how to interpret GDPR, resulting in part from the EU General Court's decision in SRB and the EDPB's forthcoming revision of its anonymization guidance. Further, Brazil's Autoridade Nacional de Proteção de Dados ("ANPD") recently conducted a public consultation on draft anonymization and pseudonymization guidance, which closed on April 3, 2024^{xvi}. How the final guidance will approach these issues is unclear, but it is notable that the draft guidance, in contrast to some interpretations of GDPR, emphasized that anonymization does not mean reducing the risk of identifiability to near-zero, but rather substantially reducing it given the context of data processing.

Taking all of these developments together, now is a ripe time in Brazil to be exploring issues surrounding PETs and anonymization. We hope that the learnings from the Open Loop program will be helpful as these policy conversations in Brazil continue to develop.

About the cohort

Nine companies participated in the Open Loop program in Brazil. This was an intentionally diverse set of companies, representing companies of varying sizes and in different sectors. Figure 1 presents more information on the companies.



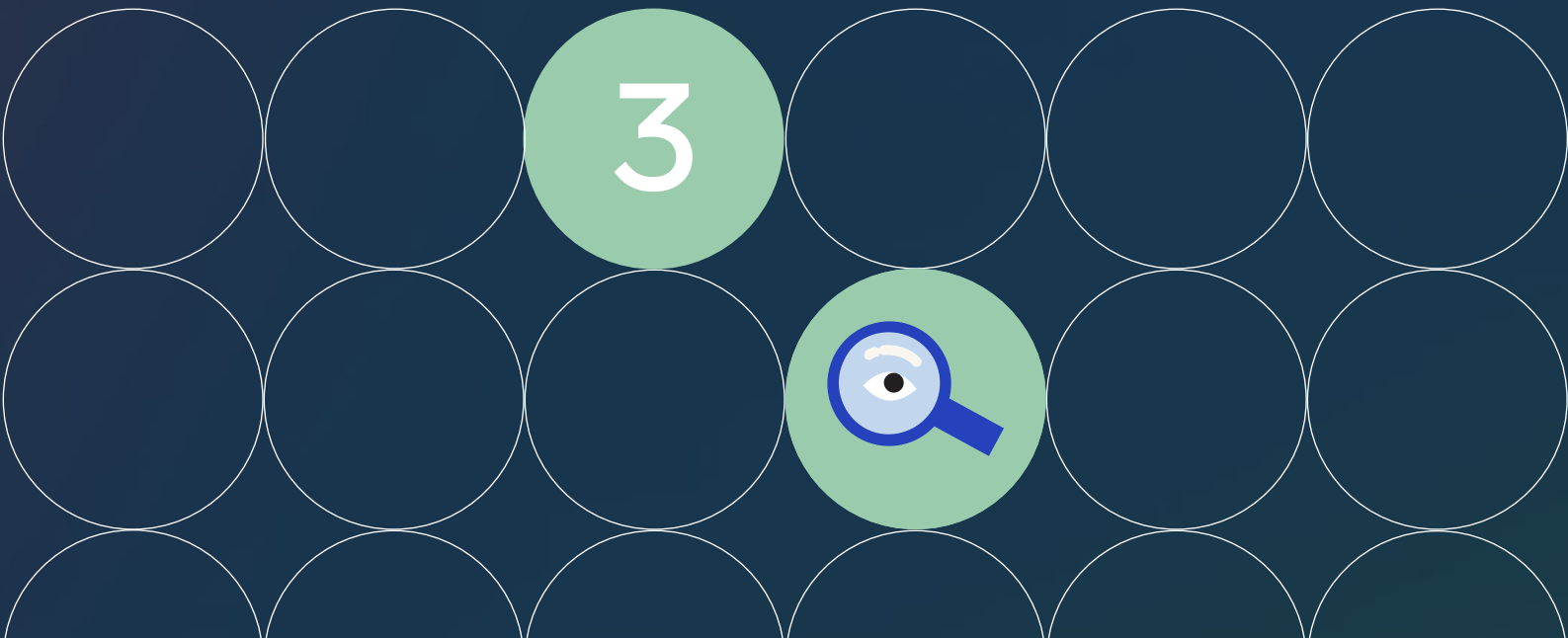
Company	Type - Sector	Business model	Size
 Antares COMUNICAÇÃO	Advertising and digital marketing	B2B	Small
	Edtech in English school franchise segment	B2B, B2C	Small
	Health	B2B, B2C	Large
	Marketplace	B2B, B2C	Large
	IT and digital marketing comms services (chatbots)	B2B	Small
	Fintech	B2B, B2C	Large
	Fintech (P2P lending)	B2B	Small
	RetailTech	B2B (SaaS)	Small
	IT Consultancy and services	B2B, B2C	Medium

Figure 1 - Participating companies. Companies were categorized according to size using OECD definitions: small (10 to 49 employees); medium (50 to 249 employees); and large (250 or more employees).

Findings

Across the Open Loop programs in Brazil and Uruguay, generally similar findings emerged. This section presents a summary of some of the most salient findings from both programs, extracting high-level themes from across research questions relating to the Playbook’s clarity, effectiveness, and feasibility. Where appropriate, any important differences in findings between countries are noted.



FINDING

3.1 Companies reported a low familiarity with PETs, especially advanced ones

DETAILS

Across both countries, there were gaps in participants' understandings of, and familiarities with, PETs at the start of the programs. But the natures of these gaps were different in the two countries. In Uruguay, at the start of the program participants were asked to rate their familiarity with PETs on a Likert-type scale ranging from zero (a complete lack of understanding) to five (a complete understanding). The average score was a 2.5, indicating a relatively low level of familiarity with PETs. In Brazil, however, many companies had at least some understanding of PETs, with nearly 80% of companies reporting that they were already using traditional PETs like anonymization or pseudonymization techniques. The same, though, was not true for more advanced PETs, suggesting a lower awareness or understanding of more advanced PETs.

FINDING

3.2 The PETs playbook helped companies to identify privacy risks and mitigation strategies

DETAILS

Participants in both countries generally found the Playbook clear and helpful. In Brazil, for example, two-thirds of companies stated that Step 1 of the Playbook was helpful for identifying potential privacy risks. Interestingly, the primary difference between these companies and those that did not find Step 1 of the Playbook helpful was likely size; all of the small companies found the Playbook's content useful, while just over a third of large companies did. Similar findings were observed in Brazil for Steps 2 and 3 of the Playbook; a majority of companies reported that Step 2 contributed in a moderate or significant way to their ability to identify privacy mitigation strategies, and 75% of companies rated the Playbook's material in Step 3 as either somewhat or extremely useful.

In Uruguay, entities reported gleaning significant learnings from the playbook. One entity said, "We gained insights about the common risks that may arise at the different stages of the data lifecycle." With respect to learning about risk mitigation measures, another entity said, "We gained clarity about certain techniques that are currently overlooked or not considered." That said, entities in Uruguay reported that Step 3—selecting PETs—was more difficult to understand due to a lack of experience with, and existing knowledge of, PETs.

3.3 Companies experienced a burden of costs and human resource constraints.

Although entities in Brazil and Uruguay found the Playbook generally helpful and easy to understand, entities faced significant challenges in the evaluation of the application of PETs they selected in Step 3. In particular, entities in both countries expressed concerns that implementing PETs—particularly more advanced ones—required significant costs. These included technical costs, such as investing in new or modified computing and data infrastructure, and human or operational costs, such as hiring and/or training additional employees.

In Uruguay, entities were surveyed about their main concerns surrounding PETs adoption, and they could list multiple concerns. Two concerns stood out as most prevalent, each being listed by six entities: “costs of implementation and maintenance” and “lack of resources.” Notably, only three entities possessed dedicated data governance teams, potentially contributing to the frequency with which these two concerns were expressed. These concerns also pushed entities in Uruguay toward adopting simpler, easier-to-implement PETs. Of the PETs from which entities could choose, two could be characterized as relatively less complex and easier to implement: de-identification techniques and cryptographic techniques. These were selected by six and seven entities, respectively. Indeed, one entity said, “De-identification may be viable for our case as it applies to any data set, and the cost of shrinking, tokenizing, hashing, or anonymizing is quite low compared to other more complex techniques. The same goes for cryptographic techniques.” The only other PETs selected by some entities were differential privacy, synthetic data, and trusted execution environments, each of which was selected by only one or two entities.

In Brazil, as mentioned earlier, most entities were already using traditional, less complex PETs like anonymization or pseudonymization techniques. But entities in Brazil nonetheless faced challenges implementing PETs, particularly more complex ones. When surveyed about their main concerns surrounding PETs adoption, 75% of entities cited implementation and maintenance costs. For some large entities, concerns often revolved around human costs—finding available engineering teams—needed to deploy both those and more advanced techniques. For example, one entity stated, “To apply PETs, it is necessary to have human resources specialized in the subject, as they are not easy to implement.”

FINDING

3.4 Regulatory uncertainty is a key barrier to PETs adoption

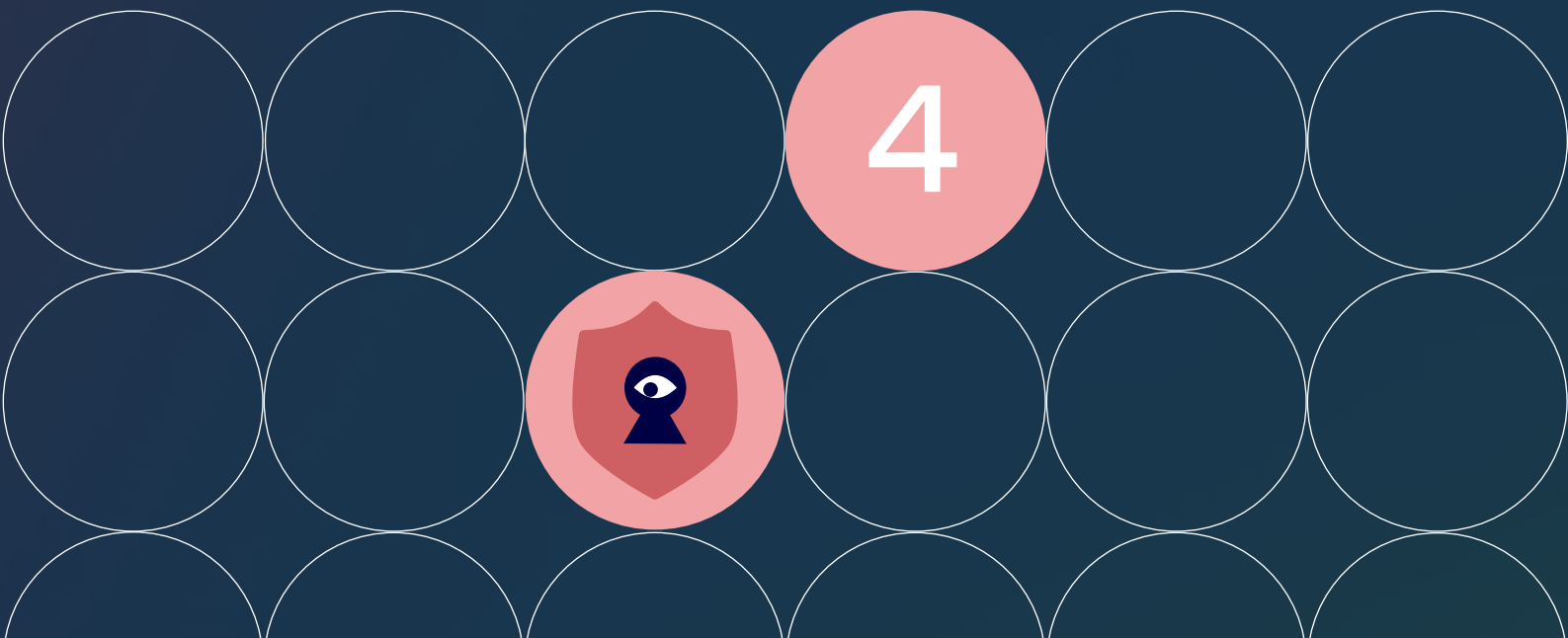
DETAILS

In addition to the costs that come with applying PETs, entities in both countries expressed a desire to use PETs to help advance data protection principles, but the exact relationship between PETs and data protection laws is unclear. In Brazil, 87.5% of entities surveyed cited the ability to meet regulatory expectations as a factor for implementing PETs, more than any other factor. In Uruguay, when entities were surveyed about their primary concerns surrounding PETs adoption, the most frequently reported concern other than costs and lack of resources was regulatory and legal barriers; four entities reported this as a concern. This uncertainty can itself create another kind of cost beyond technical and operational costs - the need for legal advice. Indeed, one entity in Uruguay noted that, in addition to infrastructure, their “main costs include . . . legal advice and possible modifications to the application to comply with privacy policies.”

Policy recommendations

Taking the Open Loop programs' results together, entities in Brazil and Uruguay are eager to deploy PETs and see their potential to advance data protection principles. But significant barriers stand in their way. Many entities—especially small and medium ones—lack existing familiarity with PETs and the technical knowledge of how to implement them. Further, implementing PETs—especially newer, more technically complex ones—comes with significant costs and uncertainties. PETs often require significant financial investments in new data infrastructure and computational power, as well as employees with relevant technical skills. Beyond these costs, entities also face significant uncertainty about how their uses of PETs relate to various provisions of data protection laws, disincentivizing costly investments in PETs.

These challenges present a prime opportunity for policymakers. Policymakers, like entities, are increasingly recognizing the value of PETs and seeking to incentivize their use. The Open Loop programs' results provide a blueprint for doing so by identifying the root causes of participants' challenges and uncertainties - causes that policymakers could seek to address. This section provides discrete, actionable recommendations that we hope will be helpful for doing so.



4.1 Regulatory certainty and incentives for PETs adoption

Policymakers around the world have the ability to draft or modify laws, regulations, or interpretations in ways that can address the regulatory uncertainty cited by participants. In particular, we would encourage policymakers to:

Embrace a flexible, risk-based approach to the legal concept of anonymization

For many entities, knowing that their uses of PETs could be deemed by regulators as legally anonymizing data is a powerful incentive. If data has been anonymized through the use of PETs, entities can do more with that data. But, as discussed previously, how different jurisdictions approach the legal concept of anonymization is unclear. Some entities, such as the UK ICO, Singapore PDPC, and IMDA have embraced what could be considered a flexible, risk-based approach. This approach recognizes that anonymization does not have to mean reducing the risk of identifiability to near zero; there can be some residual, albeit small, amount of risk. Measuring the level of risk should be a fact-specific assessment that considers the context of data processing, what technical measures (such as PETs) have been applied to the data, and what non-technical measures (such as access controls and legal restrictions) have been applied to the data. Further, as noted by the EU General Court in SRB, measuring risk could focus on whether parties who might realistically get access to the data could re-identify the data given all of the protections that have been applied to it, not whether any theoretical third party with unlimited resources and access to other data could. We would encourage policymakers to follow in the steps of the UK ICO, the Singapore PDPC and IMDA, and the EU General Court.

Clarify that entities can process data for the purpose of reducing the risk of identifiability

In addition to uncertainty over when and how using PETs can legally anonymize data, entities also face uncertainty surrounding whether their use of PETs is a justified processing of personal data in the first instance. Even though doing so is clearly aligned with the goal of data protection laws—increasing individuals' privacy—many laws fail to state that this kind of processing is permitted. We would encourage policymakers to address this deficiency. In particular, for jurisdictions that rely on GDPR-like laws—those under which a legal basis is required to process data—policymakers should clarify either that: (i) no legal basis is needed for processing data for the purpose of reducing the risk of identifiability; or (ii) legitimate interests, or a similar legal basis, can readily be relied upon to conduct such processing.

To both of these ends, we would also encourage policymakers to explore these topics more thoroughly through regulatory sandboxes. Regulatory sandboxes can provide crucial opportunities for both policymakers and entities to learn together, especially in contexts—like using PETs—that are technically complex and novel.

4.2 Multi-stakeholder dialogues around best practices and standards

In addition to providing regulatory certainty, policymakers have a valuable role to play in advancing multi-stakeholder dialogues around PETs. Open Loop program participants found great value in being able to learn from technical and policy experts about PETs, and policymakers around the world could develop similar conversations in their jurisdictions.

Not only could these conversations help to build entities' capacities to deploy PETs, but they could also make progress on developing a shared understanding of PETs and how they can be effectively used in different use cases. As discussed earlier, PETs are a diverse group of techniques that operate in very different ways and provide different kinds of privacy protections. This means that what might be considered a best practice or standard for using a PET will depend heavily on what the PET is and what context it is being deployed in. Policymakers could convene dialogues to explore these intricacies, seeking participation from standards-setting bodies and industry-wide associations in the process.

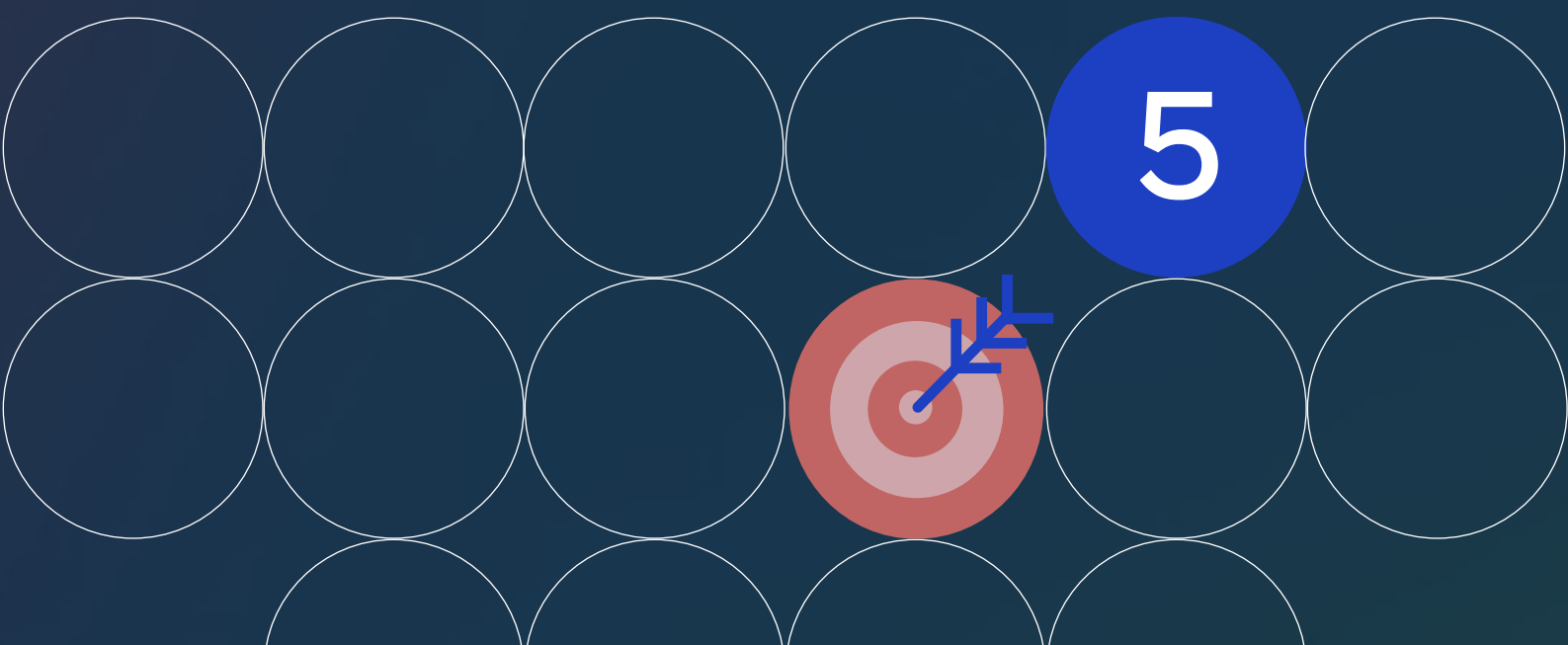
4.3 Direct investment in research, development, and education

Finally, we would encourage policymakers to invest directly in PETs research and development, as well as public education about the benefits of PETs. The results of the Open Loop programs showed that many entities—especially small and medium ones—simply lacked the resources and funding to deploy PETs at scale. This challenge could be addressed by direct government funding of R&D, as the US and UK governments did through their prize challenges, providing incentives directly to entities to develop and deploy PETs. Policymakers could also fund R&D into open-source PETs implementations, which could be more readily used off-the-shelf by small and medium entities.

In addition to R&D, policymakers could invest in public education campaigns that help explain to individuals how PETs can protect their privacy. Some entities may not pursue PETs if they feel like their customers or users would not understand the benefits of doing so, especially when deploying PETs requires great resources. But greater public awareness of PETs could address this hesitancy by making it more likely that individuals would appreciate the investments entities make in PETs.

Conclusion & next steps

In sum, the Open Loop programs in Brazil and Uruguay helped foster greater understanding of PETs and how to apply them among participating companies. The capacity building sessions and Playbook were viewed as helpful, but participants faced challenges when evaluating the implementation of PETs. For many participants, deploying PETs was viewed as a technically complicated and expensive process. And, although participants expressed a strong desire to use PETs to advance data protection principles, how exactly PETs relate to data protection laws was unclear, and legal advice on this point was yet another cost to consider. These learnings should prove valuable for policymakers, helping them craft regulations and programs that increase regulatory certainty, build multi-stakeholder dialogues, and stimulate research and development into these promising technologies



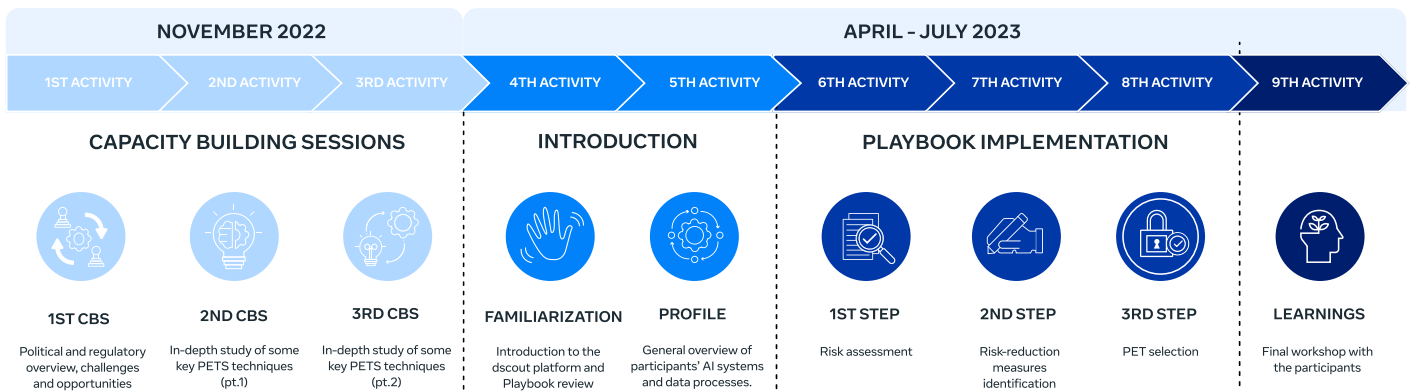
Annex 1 - Methodology

Scope

The Open Loop Brazil and Uruguay programs were guided by the following key overarching research questions:

- RQ1: How effectively does the policy prototype balance policy clarity, technical feasibility, and policy effectiveness for its intended audience?
- RQ2: What is the companies' current familiarity and understanding of PETs?
- RQ3: What are the current gaps and implementation challenges for PETs adoption by participating companies?
- RQ4: What best practices and learnings can contribute to the successful adoption of PETs to help reduce the identifiability of data and mitigate privacy-related risks?

A mix-method research methodology was employed, incorporating a combination of qualitative and quantitative methods. We collected data from different sources: desk research, interviews, surveys, and workshops. This mixed-method approach allowed us to triangulate the data and address the research questions from various perspectives (see table below).



Limitations and Considerations:

The mixed-methods approach proposed for this study is well-suited to address the research questions and objectives. However, the limitations of the methodology should be carefully considered when interpreting the findings of this report.

- Self-reported data: Reliance on self-reported information introduces potential bias, requiring cautious interpretation.
- Limited sample size: While representative of diverse industries, the sample size may not capture all industry nuances or emerging practices.
- Temporal scope: The research captured a specific point in time (from November 2022 until July 2023), and practices may evolve over time.

These limitations necessitate careful interpretation of findings. Triangulation of data from multiple sources and methods mitigates potential biases. While not generalizable to the entire population, the research provides valuable insights and trends within the participating organizations. Future research can expand the scope and address emerging practices.

References

- ¹ Del Pozo, C., Nuno Gomes de Andrade, N., & Rojas Arroyo, D. "Prototipo de Políticas Públicas sobre Transparencia y Explicabilidad de Sistemas de Inteligencia Artificial [Public Policy Prototype on the Transparency and Explainability of Artificial Intelligence Systems] (2023), at: <https://openloop.org/reports/2023/10/Public-Policy-Prototype-on-the-Transparency-and-Explainability-of-Artificial-Intelligence-Systems.pdf>
- ² OECD (2023). "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, <https://doi.org/10.1787/bf121be4-en>.
- ³ National Science and Technology Council (2023). National Strategy to advance privacy-preserving data sharing and analytics, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf>
- ⁴ The White House (2023, October 30). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The White House. <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>
- ⁵ Near, J., Darais, D., Lefkovitz, N., & Howarth, G. (2023, December 11). Guidelines for Evaluating Differential Privacy Guarantees. <https://csrc.nist.gov/pubs/sp/800/226/ipd>
- ⁶ Privacy Enhancing Technology Research Act, no. 4755, Science, Space, and Technology (2023). <https://www.congress.gov/bill/118th-congress/house-bill/4755>
- ⁷ Information Commissioner's Office (2023, June 19). Privacy-enhancing technologies (PETs). Information Commissioner's Office. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/>
- ⁸ U.K.-U.S. prize challenges | Privacy-Enhancing Technologies. [Petsprizechallenges.com](https://petsprizechallenges.com). Retrieved May 2, 2024, from <https://petsprizechallenges.com/>
- ⁹ European Data Protection Board (2023). EDPB Work Programme 2023/2024. https://www.edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf
- ¹⁰ SRB v. EDPS, (Court of Justice of the European Union April 26, 2023). https://gdprhub.eu/index.php?title=CJEU_-_Case_T-557/20_-_SRB_v._EDPS#:~:text=EDPS,-From%20GDPRhub&text=The%20European%20General%20Court%20ordered,alphanumeric%20codes%20constituted%20personal%20data.
- ¹¹ Infocomm Media Development Authority. Privacy Enhancing Technology Sandboxes. Retrieved May 2, 2024, from <https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes>
- ¹² Infocomm Media Development Authority. Digital Advertising in a Paradigm Without 3rd Party Cookies. Retrieved May 2, 2024, from <https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--meta.pdf>
- ¹³ Kwon, S. (2024, February 2). In the era of artificial intelligence, standards for pseudonym processing for images, videos, voices, and texts have emerged. <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttlId=989>
- ¹⁴ OECD (2023).
- ¹⁵ UN Committee of Experts on Big Data and Data Science for Official Statistics. Task Team on Privacy Preserving Techniques — UN GWG for Big Data. [unstats.un.org](https://unstats.un.org/bigdata/task-teams/privacy/index.cshtml). Retrieved May 2, 2024, from <https://unstats.un.org/bigdata/task-teams/privacy/index.cshtml>
- ¹⁶ Autoridade Nacional de Proteção de Dados (ANPD). (2024, February 28). Prorrogadas consultas sobre guia de anonimização e norma de direitos dos titulares. Retrieved from <https://www.gov.br/anpd/pt-br/assuntos/noticias/prorrogadas-consultas-sobre-guia-de-anonizacao-e-norma-de-direitos-dos-titulares>