FUTURE OF PRIVACY FORUM

APRIL 2022

Privacy Tech Buyer Framework

AUTHORED BY

Tim Sparapani and Justin Sherman

for the Future of Privacy Forum

ACKNOWLEDGMENTS

The authors would like to thank all of the members of the Privacy Tech Alliance (https://fpf.org/privacy-tech-alliance) who participated in the many working group sessions that led to this report. The authors would also like to thank all of the individuals, on both the buy and sell sides of the process, who spoke with them for the previous *Privacy Tech's Third Generation* report and whose insights helped inform this report. Finally, the authors would like to thank the Future of Privacy Forum's Jules Polonetsky, John Verdi, and Amanda Browe, as well as Katharina Koerner, formerly of FPF and now at the International Association of Privacy Professionals, for their support.

FUTURE OF
PRIVACY
FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org**.**

Privacy
Tech
Alliance

The Future of Privacy Forum launched the **Privacy Tech Alliance (PTA)** as a global initiative with a mission to define, enhance, and promote the market for privacy technologies. The PTA brings together innovators in privacy tech with customers and key stakeholders.

EXECUTIVE SUMMARY FOR BUSINESS USERS

The Privacy Tech Buyer Framework is a tool to help you and your business buy the best privacy technology or privacy service to achieve your business outcomes. Buying the appropriate tool or service can be challenging, so the Privacy Tech Alliance Working Group has built this Framework to simplify and clarify the buying process.

To use this Framework, you need only ask yourself three simple questions:

1. What business outcomes do I want to achieve?
2. What categories of privacy technologies can best help me achieve my preferred outcome?
3. What specific privacy technologies might best suit my needs?

The Privacy Tech Alliance Working Group Framework walks you through why this is the best way to make your purchasing decisions. We hope we have helped make a complicated decision process less complex.

INTRODUCTION

The global privacy technology market is rapidly evolving. Driven by new regulatory demands, contractual requirements with customers, and slowly emerging recognition of the reputational risks of data privacy breaches (broadly defined), the sector has moved from offering narrow compliance-specific tools to offering more integrated, diverse technologies to enable a range of business outcomes. In the inaugural Privacy Tech Alliance report (https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf) from the Future of Privacy Forum, this stage of evolution was defined as privacy tech's third generation.[1]

As the number of privacy tools and services available to businesses increases, so has buyer confusion about which offerings are most useful for their business needs—and some businesses may not recognize ways they can use privacy technologies in the first place. Thus, despite all these advancements, the privacy tech market can be challenging for buyers to navigate. In particular, interviews of buyers and ongoing discussion with vendors in the Privacy Tech Alliance continue to make clear there is a lack of consistent, consensus privacy tech terminology among and between buyers and sellers. This limits understanding of vendor offerings and buyer needs: different terms can be used for the same technologies, and the same terms can be used in entirely different ways. Relatedly, privacy tech buyers may also have difficulties identifying business outcomes that can be achieved with or supported by privacy technologies. Unaddressed, this misalignment and misunderstanding will slow the privacy tech industry's long-run growth.

As a business, deciding to purchase a privacy technology can be a complex process. There are numerous privacy technologies and services in the market, each with their own terminology and use cases. New businesses and product offerings are cropping up each year. Some of these technologies are designed to plug-and-play into any business IT environment, while others require custom installation or might function more easily in some IT environments compared to others. On top of all that, a business may face different regulatory demands depending on where they operate and the data they handle, and different stakeholders within a business may want to purchase a privacy technology for different reasons. Businesses looking to acquire privacy technologies are faced with many considerations.

This Privacy Tech Buyer Framework therefore offers guidance for buyers to navigate the privacy tech acquisition process. The framework breaks the decision process down into three phases, each involving a series of questions—where the decision process begins with a higher-level assessment of buyer needs (and potentially unrecognized buyer needs), and then moves towards operationally pairing those needs with specific kinds of privacy technologies. Throughout this process, it guides the user towards the eventual decision of what tools and services to purchase from privacy tech vendors.

It is important to state what this framework is not. It is not marketing material for one or a series of companies. It is not intended to speak to all businesses' needs for every privacy or security purchase, and it is not intended to be comprehensive. It is not meant to, nor can it, replace the guidance of legal counsel or fully explain how buyers can comply with data privacy regulatory, statutory, or contractual requirements or similar data security requirements. The framework also covers privacy technologies and does not focus on technologies more often considered part of the cybersecurity domain, such as network firewalls and antivirus software. While there is overlap between privacy and security, as with the confidentiality of individuals' sensitive information, this report focuses primarily on privacy technologies unrelated to unauthorized system access and behavior.[2]

This report is a gap-filling document meant to bridge the chasm uncovered during more than 50 hours of interviews with privacy tech buyers and vendors—and supported by many hours of subsequent conversation between the authors and Privacy Tech Alliance working group members. It is meant to aid buyers in identifying what tools and services are available to help their businesses responsibly and legally use personal information to meet business needs and achieve business outcomes, as typical of privacy tech's third generation. This document additionally recognizes that those buyers also need a common language to work from, along with a process for analyzing their business' needs and vendors' ability to respond to those needs.

To solve these problems, Privacy Tech Alliance working group members convened and built the Privacy Tech Buyer Framework, which breaks down the privacy tech acquisition process into three phases.

- First, buyers must understand the business outcomes they are trying to achieve.
- Second, buyers must match those desired outcomes to categories of privacy tech products.
- Third, within those categories of privacy tech products, buyers must identify tools and services that will fulfill those outcomes and begin to identify vendors that provide those tools and services.

THE PRIVACY TECH BUYER FRAMEWORK

This framework is designed to help businesses navigate the privacy tech acquisition process. It breaks this decision down into three phases, moving through a series of questions to identify the appropriate privacy tech tools or services to obtain. This decision process begins with higher-level business outcomes in Phase 1 and ends with business-friendly privacy tech definitions in Phase 3. Its structure and content draw on numerous meetings of the Privacy Tech Alliance working group and the group members' experiences as providers of tools and services to customers. Additionally, the framework draws from the Future of Privacy Forum/ Privacy Tech Alliance report *Privacy Tech's Third Generation*, and existing frameworks from the U.S. National Institute of Standards and Technology and other organizations.

Phase 1 — Business Outcomes

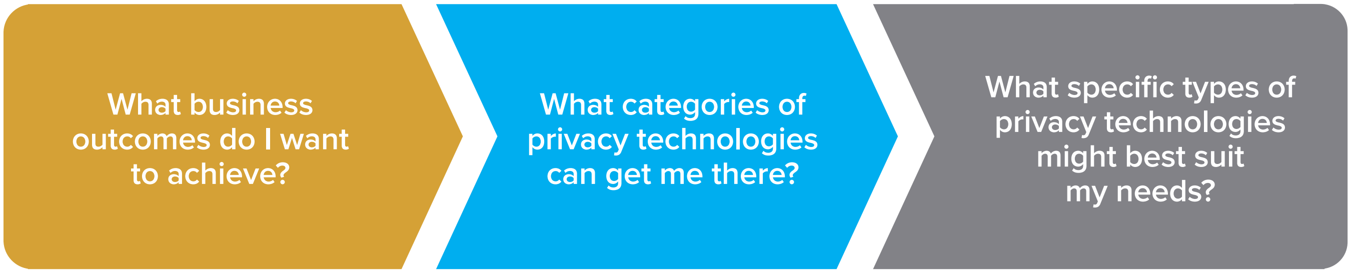
(aka Privacy Tech 3.0)

The first and most important step in a buyer's privacy tech acquisition process is understanding what business outcomes they are trying to achieve. These desired business outcomes may be different for different businesses, and they may also vary between stakeholders in a single organization (from Chief Privacy Officers to marketing professionals). All of those factors will affect which privacy technologies are best suited for the business' needs.

The following categories of business outcomes that can be aided or achieved with privacy technologies draw from the Future of Privacy Forum/Privacy Tech Alliance's *Privacy Tech's Third Generation* report,[3] which was developed from research on the privacy tech market, dozens of hours of interviews with privacy tech buyers and sellers, and a survey distributed to privacy technology companies:

- **Data availability and movability:** Chief Information Officers and other technology personnel ensuring data is readily available for use and is quickly and reliably transferred around the world or localized as needed
- **Information security for people and assets:** Chief Information Security Officers and other information security personnel ensuring data's confidentiality, integrity, and availability [not the focus of this report]
- **Data value creation/analysis:** Chief Data Officers, Chief Marketing Officers and their marketing teams, and other data science personnel ensuring data generates and can be used to generate (e.g., through analysis) value for the business
- **Data protection as ethics, compliance, and mitigation:** General Counsels, Chief Privacy Officers, Chief Ethics Officers, legal teams, DPOs, and other compliance personnel ensuring data is legally collected, stored, transferred, and otherwise processed based on applicable regulations—and that data risks are mitigated

The Privacy Tech Buyer Framework: Simplified Steps

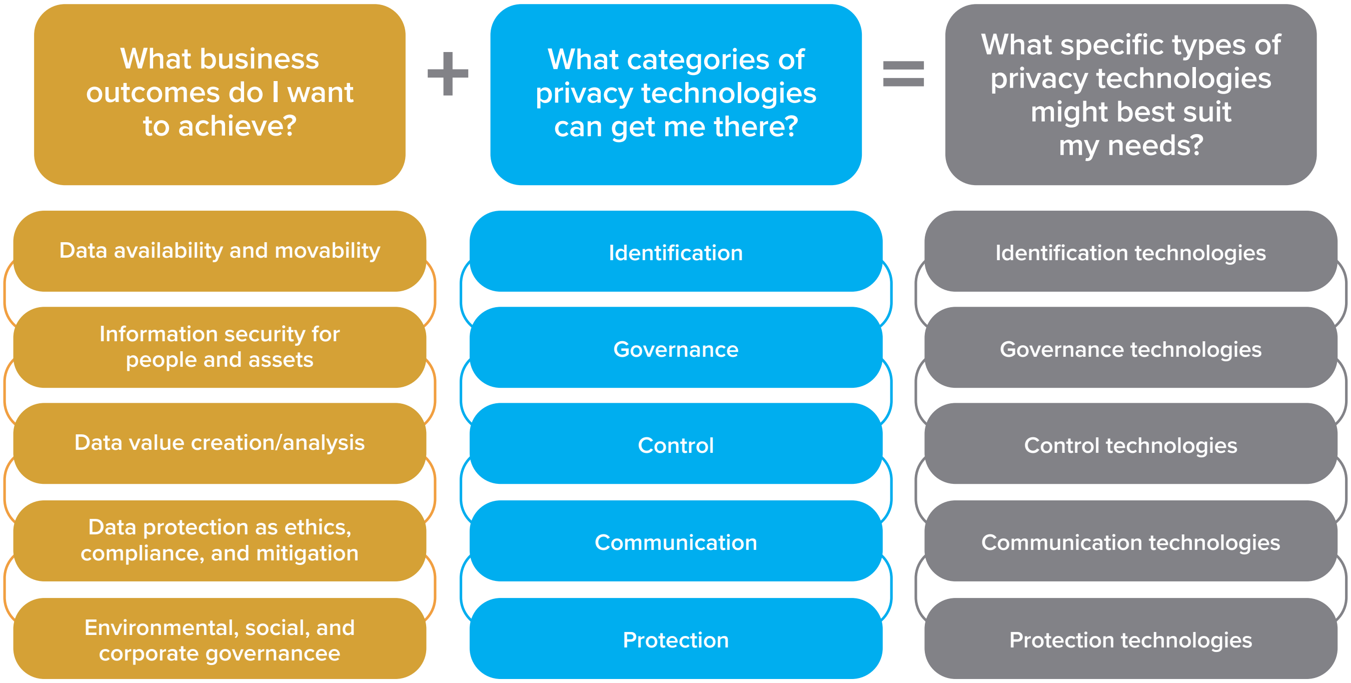


What business outcomes do I want to achieve?

What categories of privacy technologies can get me there?

What specific types of privacy technologies might best suit my needs?

The Privacy Tech Buyer Framework: Full Steps



What business outcomes do I want to achieve?	+	What categories of privacy technologies can get me there?	=	What specific types of privacy technologies might best suit my needs?
Data availability and movability		Identification		Identification technologies
Information security for people and assets		Governance		Governance technologies
Data value creation/analysis		Control		Control technologies
Data protection as ethics, compliance, and mitigation		Communication		Communication technologies
Environmental, social, and corporate governancee		Protection		Protection technologies

And, looking forward:

- **Environmental, social, and corporate governance:** Investors, board members, and corporations in general increasingly making environmental, social, and governance factors a business priority, including the protection of data

Buyers may also want to consider the data relationships in question (e.g., sharing data internally, sharing data with an external contractor, etc.) as well as identify what other considerations—including data accuracy, performance, scalability, and generality—might be most important for their objectives. There may be trade-offs between these considerations.

Phase 2 — Product Category Descriptions

(high-level privacy tech taxonomy)

Once a buyer identifies the business outcomes they want to achieve (and relevant business requirements), the next step in the privacy tech acquisition process is matching business outcomes to categories of privacy technology products. Understanding which categories of privacy technologies can help with which business outcomes, and how those categories of technologies may overlap or interact with one another, can help buyers more quickly identify which kinds of privacy technologies to pursue.

The following categories of privacy tech products draw on the U.S. National Institute of Standards and Technology (NIST)'s Privacy Framework,[4] with language adapted to refer specifically to privacy technologies:

- **Identification:** privacy technologies used to understand the data a business collects, processes, analyzes, and stores on individuals
- **Governance:** privacy technologies used to develop and implement the organizational governance structure to continuously understand a business' risk management priorities that are informed by privacy risk

- **Control:** privacy technologies used to develop and implement activities to enable a business to manage data with sufficient granularity to manage privacy risks
- **Communication:** privacy technologies used to enable a business to have a reliable understanding and engage in dialogue with individuals about how data is processed and associated privacy risks
- **Protection:** privacy technologies used to develop and implement appropriate data processing safeguards

Phase 3 — Focus on Business-Level Tools and Services

(secondary level privacy tech taxonomy; these tools support the outcomes)

After pairing categories of privacy technology products with business outcomes, buyers are one step closer to identifying privacy technologies for potential acquisition. Before identifying specific products and services from specific vendors, however, buyers must decide which categories of functions that privacy technologies might fall into.

The following categories of business-level tools and services draw on and are adapted from the U.S. National Institute of Standards and Technology (NIST)'s Privacy Framework,[5] with language modified to refer specifically to privacy technologies:

- **IDENTIFICATION**
  - **Inventory and Mapping:** privacy technologies used to identify and map data processed from a business' systems, products, and services; also used to understand and inform privacy risk management
  - **Business Environment:** privacy technologies used to understand and prioritize a business' mission, objectives, stakeholders, and activities in order to inform privacy roles, responsibilities, and risk management decisions
  - **Risk Assessment:** privacy technologies used to understand privacy risks to individuals and how those risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture
  - **Data Processing Ecosystem Risk Management:** privacy technologies used to establish an organization's priorities, constraints, risk tolerance, and assumptions, in order to support privacy risk management decisions and third parties within the business' data processing ecosystem
- **GOVERNANCE**
  - **Governance Policies, Processes, and Procedures:** privacy technologies used to manage, monitor, and generate the policies, processes, and procedures for a business' regulatory, legal, risk, environmental, and operational requirements, in order to understand and inform privacy risk management
  - **Risk Management Strategy:** Privacy technologies used to establish and communicate a business' priorities, constraints, risk tolerances, and assumptions around operational risk decisions
  - **Awareness and Training:** privacy technologies used to provide privacy awareness education to the business and third parties engaged in data processing, and to train those organizations to perform their privacy-related duties and responsibilities consistent with related policies,

processes, procedures, and agreements and organizational privacy values

- **Monitoring and Review:** privacy technologies used to understand a business' policies, processes, and procedures as part of the ongoing review of privacy risk

› CONTROL

- **Data Processing Policies, Processes, and Procedures:** privacy technologies used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the business' risk strategy to protect individuals' privacy
- **Data Processing Management:** privacy technologies used to manage data consistent with the business' risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization)
- **Disassociated Processing:** privacy technologies used to increase disassociability consistent with the business' risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization)

› COMMUNICATION

- **Communication Policies, Processes, and Procedures:** privacy technologies used to maintain policies, processes, and procedures and to increase the transparency of the business' data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks; conversely, also includes technologies that enable consumers to provide consent, make data collection opt-out requests, make data access requests, make data deletion requests, and otherwise communicate with the business
- **Data Processing Awareness:** privacy technologies for the business and/or individuals to reliably understand data processing practices and associated privacy risks and for the business to increase predictability consistent with its risk strategy to protect individuals' privacy

› PROTECTION

- **Data Protection Policies, Processes, and Procedures:** privacy technologies used to maintain privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures in order to protect data
- **Identity Management, Authentication, and Access Control:** privacy technologies used to limit access to data and devices to authorized individuals, processes, and devices, managed consistently with the risk of unauthorized access
- **Data Security:** privacy technology used to ensure data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability
- **Maintenance:** privacy technologies used to perform system maintenance and repairs, consistent with policies, processes, and procedures
- **Protective Technology:** privacy technologies used to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements

CASE STUDIES

This section includes a number of case studies, submitted by Privacy Tech Alliance working group members, to illustrate just some hypothetical scenarios in which a buyer may use the Privacy Tech Buyer Framework to move from a general business outcome—and open questions about their privacy technology needs—towards a specific buy decision.

CASE STUDY: Media Company Advertising

OVERVIEW. The Buyer company is a major media company that owns a network of digital web and mobile news publications. Buyer relies heavily on programmatic advertising for its revenue and therefore has relationships with multiple partners to serve advertising on its media properties. Buyer used the Buyer Framework to identify what privacy technologies are best suited for its business needs with respect to their media properties.

PHASE 1 — Business Outcomes. After meeting with stakeholders, Buyer identified two business outcomes that Buyer would like to achieve from use of privacy technologies:

- **Data value creation/analysis**. In order to monetize Buyer's media properties, Buyer wants to ensure that data about visitors to Buyer's properties can be effectively collected and used by Buyer and its adtech partners to target, measure and optimize the value of advertisements on Buyer's properties, without sacrificing user experience.
- **Data protection as ethics, compliance and mitigation**. Buyer's General Counsel, Chief Privacy Officer, Chief Ethics Officer, legal team and other compliance personnel want to ensure data collected from Buyer's media properties is legally collected and processed by both Buyer and its third-party partners and that associated data risks are mitigated.

PHASE 2 — Product Categories. After identifying Buyer's desired business outcomes, Buyer used the Buyer Framework to identify the following categories of privacy technologies to pursue:

- **Identification.** Buyer needed a privacy technology to understand what data is collected from Buyer's media properties, who is collecting it, how it is processed and used, and risks associated with such data collection and use.
- **Communication.** Buyer needed a privacy technology to enable Buyer to engage in dialogue with visitors to Buyer's media properties in order to be transparent about what data is collected, by what entities, and for what purposes and to enable users to exercise their legal rights and express their preferences with respect to such data collection.
- **Control.** Buyer needed a privacy technology to develop and implement activities to manage the collection of data from visitors to its media properties with sufficient granularity to manage privacy risk, based on user preferences and the knowledge of data and risk gained through the identification category above.

PHASE 3 — Business-Level Tools and Services. After pairing categories of privacy technology products with Buyer's business outcomes, Buyer decided that the following categories of business-level tools and services would best suit Buyer's needs:

- **Inventory and Mapping.** Buyer needed a privacy technology to help: (a) Buyer to understand what data is collected from its media properties, how it is processed and by whom; and (b) inform Buyer's management of privacy risk from such data collection and use.
- **Data Processing Ecosystem Risk Assessment.** Buyer needed a privacy technology to help Buyer identify, assess and manage privacy

risks within the programmatic advertising ecosystem with respect to the processing of data collected from Buyer's media properties.

- **Data Processing Awareness.** Buyer needed a privacy technology to ensure visitors to the media properties have reliable knowledge about Buyer's and its third party partners' data processing practices and associated privacy risks, and that effective mechanisms are used to capture user preferences in order to increase predictability for the user and all data processors involved, consistent with the organization's risk strategy to protect individuals' privacy.
- **Data Processing Policies, Processes, and Procedures.** Buyer needs a privacy technology to manage data processing on its media properties based on identified data collection, identified risks, and user preferences learned in the previous three steps, consistent with the business' risk strategy to protect individuals' privacy.

CASE STUDY: Randomized Healthcare Surveying

OVERVIEW. A set of healthcare organizations form a consortium to share patient data in an effort to monitor the spread of diseases within a community, and determine potential risk factors for contracting severe illness. This will be done by surveying and sharing de-identified patient records between consortium members.

PHASE 1 — Business Outcomes. The two main business outcomes of the consortium are thus data value creation/analysis and data protection as compliance, ethics, and mitigation.

PHASE 2 — Product Categories. The consortium is interested in implementing PETs that will achieve dissociation. In turn, it pinpoints Identification and Control as two important categories of privacy tech products.

PHASE 3 — Business-Level Tools and Services. To select the right privacy-enhancing techniques (PET), the operation team of the consortium further breaks down the dissociation goal and identifies the following subcategories: indistinguishability and deniability. It then uses this information to identify specific subcategories within the Identification and Protection categories, including Data Processing Ecosystem Risk Management (Identification) and Data Processing Management (Control).

Context on the technology. In order to achieve indistinguishability, all publicly available direct identifiers are removed from the shared data and all publicly available indirect identifiers are obscured using a K-anonymization PET.

Though all publicly linkable attributes have been obscured such that no single record can be unambiguously associated with a patient, this does not guard against inferring ubiquitous diseases within a population of patients. If all or most of the patients within a cohort have a common disease diagnosis, an attacker could confidently infer that any patient within a clinic is positive for that disease. The operation team thus decides to implement an attribute randomization PET to inject uncertainty to any conclusions an attacker could draw and enable members of the community to deny the value of sensitive attributes, i.e., to achieve deniability.

Randomization is done by first selecting a target replacement rate ($R_{Replace}$). Then two random numbers, each bound between [0, 1) are generated: one for perturbation (r_p) and a second for selection (r_s). If r_p is less than one minus the target replacement rate, then the true diagnosis is revealed. Otherwise a diagnosis is revealed by randomly selecting, with uniform probability over the list of other possible diagnoses, using the second random number r_s. For example, consider the available ICD-10 codes for a subset of diagnoses: I10 (Essential Hypertension), R7303 (Prediabetes), H5710 (Ocular pain), and Z21 (Asymptomatic HIV Infection). The patient has a positive diagnosis for hypertension (I10). If r_p is less than 1-Replacement Rate, the true diagnosis (I10) is revealed. Otherwise, one of the three other diagnoses are revealed:

The attacker *knows* that some fraction of the responses are incorrect, in fact the attacker should be informed of the replacement rate. That way the attacker is not confident that the response they are seeing is a true response or produced by a randomizer.[6]

The simplicity of this relation means that an attacker can recover an estimate of the true distribution fairly simply, provided that the replacement rate is somewhat less than 1-1/N, where N are the size of the domain. In the example above, the domain would be 4. At the same time, the attacker is prevented from knowing the accuracy of any single response.

By being able to deconvolve the noise induced by the randomizer, an observer or attacker, e.g. an analyst sitting in the consortium data science team, can still gain meaningful insights from aggregating data, while also being unable to state with confidence that any single response is accurate or randomized.

CASE STUDY: Government Research Disclosures

OVERVIEW. A government agency manages hundreds of millions of personal records from individuals. They need to be able to release statistical summaries to other government agencies and the public, in order to further research and support evidence-based policymaking. However, these releases must adhere to stringent privacy regulations encoded in U.S. law.

PHASE 1 — Business Outcomes. The business outcome is sharing data with an external partner, while respecting privacy regulations and avoiding reputational and financial risk of a privacy attack.

PHASE 2 — Product Categories. They need a privacy-preserving transformation of the data.

PHASE 3 — Business-Level Tools and Services. Differential privacy is the best technology for this use case. Other protective methods such as de-identification, anonymization, masking, or simple aggregation combined with suppression have all led to privacy attacks and have limitations in how privacy risk can be tracked across multiple releases.

Context on the technology. To deploy differential privacy, they need software to calculate the statistical summaries they will release, add carefully calibrated noise, and fulfill the formal guarantee of differential privacy. In preparation for the release, they may also need help in configuring the level of privacy risk and trading off that risk against the accuracy of the released data.

CASE STUDY: Company Product Development

OVERVIEW. A company is developing a product and wants to have the right privacy safeguards in place.

PHASE 1 — Business Outcomes. Data availability and movability.

- Led by CIO
- Supporting product development and improvement through the sharing of real data captured from users or about users
- For analytically driven products, need to maintain real distribution of entries to explore normal behavior and outliers (testing for product failures or error handling)

PHASE 2 — Product Categories. Protection.

- wPredictability needed to ensure personal data is excluded from product development while maintaining ability to provide useful, real looking data

PHASE 3 — Business-Level Tools and Services. Disassociated processing.

- Minimizing data to attributes of interest, removing directly identifying information through masking, resynthesizing attribute values of indirectly identifying information while maintaining distributions
- Using technical privacy models[7] to ensure transformations appropriately minimize exposure and drive suitable degree of disassociation

CASE STUDY: Drug Discovery Pipeline

OVERVIEW. A company is developing a data pipeline to improve its drug discovery process.

PHASE 1 — Business Outcomes. Data value creation/analysis.

- Led by executive data leaders (CDO, VP data)
- Building a robust data infrastructure to merge source systems inside and outside of a data lake
- Developing a findable, accessible, interoperable, and reusable (FAIR) data ecosystem so that data scientists can access data they need for drug discovery
- Equipped with artificial intelligence, the system provides scientists with novel ways of interacting with data and each other
- Data and transparency leaders in the pharma industry are increasingly embracing the digital shift toward reusing clinical trial data for new benefits, including future trial design

PHASE 2 — Product Categories. Identification; Control.

- Enabling the organization to manage data with sufficient granularity to manage privacy risks
- Exploring range of access and sharing models to enable discovery, e.g., internal use, reuse of harmonized data across various sources, collaboration with other scientists in different departments or organizations, transparency of non-proprietary and non-personal data needed for public policy
- Creating safe data environments with predictable access and data sharing pipelines so that users have trustworthy means of harnessing data and collaborating

PHASE 3 — Business-Level Tools and Services. Risk Assessment; Disassociated Processing.

- Risk management / risk assessment technology used to focus efforts and determine appropriate granularity of data based on defined purposes and desired usefulness
- Disassociated processing through pseudonymized linking, secure and automated data harmonization, and integrated anonymization technology in a pipeline to serve the FAIR data ecosystem
- The anonymization pipeline includes integrated manageability to ensure different use cases can be rapidly served, with controls for alteration, selective sharing, and deletion

APPENDIX A: NIST FRAMEWORK REFERENCES

Categories from NIST Privacy Framework[8], drawn on for Phase 2:

- **Identification:** "Develop the organizational understanding to manage privacy risk for individuals arising from data processing."
- **Governance:** "Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk."
- **Control:** "Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks."
- **Communication:** "Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks."
- **Protection:** "Develop and implement appropriate data processing safeguards."

Categories from NIST Privacy Framework, drawn on for Phase 3:

- **IDENTIFICATION**
  - **Inventory and Mapping:** "Data processing by systems, products, or services is understood and informs the management of privacy risk."
  - **Business Environment:** "The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions."
  - **Risk Assessment:** "The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture."
  - **Data Processing Ecosystem Risk Management:** "The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem."
- **GOVERNANCE**
  - **Governance Policies, Processes, and Procedures:** "The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk."
  - **Risk Management Strategy:** "The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions."
  - **Awareness and Training:** "The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values."
  - **Monitoring and Review:** "The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk."

› CONTROL

- **Data Processing Policies, Processes, and Procedures:** “Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization’s risk strategy to protect individuals’ privacy.”
- **Data Processing Management:** “Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).”
- **Disassociated Processing:** “Data processing solutions increase disassociability consistent with the organization’s risk strategy to protect individuals’ privacy and enable implementation of privacy principles (e.g., data minimization).”

› COMMUNICATION

- **Communication Policies, Processes, and Procedures:** “Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.”
- **Data Processing Awareness:** “Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.”

› PROTECTION

- **Data Protection Policies, Processes, and Procedures:** “Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.”
- **Identity Management, Authentication, and Access Control:** “Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.”
- **Data Security:** “Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy and maintain data confidentiality, integrity, and availability.”
- **Maintenance:** “System maintenance and repairs are performed consistent with policies, processes, and procedures.”
- **Protective Technology:** “Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.”

APPENDIX B: SAMPLE OF BUSINESS-FRIENDLY PRIVACY TECHNOLOGY DEFINITIONS

Below is a sample list of business-friendly privacy technology definitions designed to aid buyer comprehension and, where useful, provide non-legal, non-technical definitions of tools and services that have not already been supplied by other efforts.

Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis (London: Royal Society, March 2019), https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf, p. 8-9:

- Trusted Execution Environments
  - **Type of privacy:** “Securely outsourcing to a server, or cloud, computations on sensitive data”
  - Privacy risk addressed: “Revealing sensitive attributes present in a dataset”
- Homomorphic Encryption
  - **Type of privacy:** “Securely outsourcing specific operations on sensitive data”; “Safely providing access to sensitive data”
  - Privacy risk addressed: “Revealing sensitive attributes present in a dataset”
- Secure Multi-Party Computation
  - **Type of privacy:** “Enabling joint analysis on sensitive data held by several organizations”
  - **Privacy risk addressed:** “Revealing sensitive attributes present in a dataset”
- Differential Privacy
  - Type of privacy: “Organization releasing statistics or derived information—generally an organization that holds a large amount of data”
  - **Privacy risk addressed:** “Dataset or output disclosing sensitive information about an entity included in the dataset”
- Personal Data Stores
  - **Type of privacy:** “Individual managing with whom and how they share data”; “De-centralizing services that rely on user data”
  - **Privacy risk addressed:** “Undesired sharing of sensitive information”

Cem Dilmegani, “Top 10 Privacy Enhancing Technologies (PETs) & Use Cases,” Research. AIMultiple.com, October 21, 2021, https://research.aimultiple.com/privacy-enhancing-technologies/

- Common types of PETs:
  - Cryptographic algorithms—homomorphic encryption (partial homomorphic, somewhat homomorphic, and fully homomorphic), secure multi-party computation, differential privacy, zero-knowledge proofs
  - Data masking techniques—obfuscation, pseudonymization, data minimization, communication anonymizers
  - With the help of AI and ML algorithms—synthetic data generation, federated learning
- Top PETs use cases—test data management, financial transactions, healthcare services, facilitating data transfer between multiple parties including intermediaries

APPENDIX C: OTHER RESOURCES

Gilbert & Tobin, “A guide to privacy enhancing technologies (PETs) and how to adopt them,” GTLaw.com.au, August 24, 2021, https://www.gtlaw.com.au/knowledge/guide-privacy-enhancing-technologies-pets-how-adopt-them

Clarip, “Buying Privacy Software: The 10 Categories of Privacy Technology for Business,” Clarip.com, accessed October 2021, https://www.clarip.com/data-privacy/privacy-software-categories/

ENDNOTES

[1] Tim Sparapani and Justin Sherman, *Privacy Tech’s Third Generation: A Review of the Emerging Privacy Tech Sector* (Washington, D.C.: Future of Privacy Forum, June 2021), https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf.

[2] For more on the relationship between privacy and security, see, e.g., U.S. National Institute of Standards and Technology. Sean Brooks et al. *An Introduction to Privacy Engineering and Risk Management in Federal Systems.* Gaithersburg: National Institute of Standards and Technology, January 2017. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. 7–9.

[3] *Privacy Tech’s Third Generation.*

[4] U.S. National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management.* Gaithersburg: U.S. National Institute for Standards and Technology, January 2020. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf. 20-27.

[5] Ibid.

[6] The randomization process does impact the observed data. Since the randomized responses are uniformly distributed, the observed distribution can be modeled as the sum of the distribution of truthful responses and a uniform distribution.

[7] Wagner I, Eckhoff D. Technical Privacy Metrics: A Systematic Survey. *ACM Computing Surveys.* 2018 Jun 12;51(3):57:1-57:38.

[8] https://www.nist.gov/privacy-framework/privacy-framework

NOTES

NOTES

FUTURE OF PRIVACY FORUM