Hype Cycle for Privacy, 2020

Published: 23 July 2020 **ID:** G00441605

Analyst(s): Bernard Woo, Bart Willemsen

Security and risk management leaders managing technology, information and resilience risk must consider privacy a top priority. Laws and privacy-preserving technologies that protect business value and build trust with individuals are covered in depth to support prioritization of risk and investment.

Table of Contents

List of Tables

List of Figures

Strategic Planning Assumptions

Through 2022, privacy-driven spending on compliance tooling will break through to more than $8 billion worldwide.

By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, which is a significant increase from 10% today.

Before year-end 2023, more than 80% of companies worldwide will be facing at least one privacy-focused data protection regulation.

Analysis

What You Need to Know

This document was revised on 2 October 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Privacy as a fundamental human right continues to be enshrined through regulatory changes worldwide. Where regulations do not yet exist, customers are actively choosing to engage with organizations that respect privacy. Laws inform strategy and policy, carefully applied technology enables purposeful processing, and risk management balances innovation with compliance. Privacy protection demands the deliberate control of personal data throughout its life cycle.

Security and risk management (SRM) leaders face an abundance of requirements and diverging stakeholder opinions. Some organizations prioritize privacy as a corporate value. Others may only

move following legal precedents, and there are those who believe that individuals should have little to no expectation of privacy. This challenge is exacerbated by exponential growth in data collection and analytics capabilities, and the evolution in artificial intelligence (AI) capabilities that have unearthed previously hidden sources of value within that data.

The continued maturation in the regulatory environment has driven innovative and built-for-purpose solutions. The application of new technology, such as differential privacy and homomorphic encryption, may provide a path to protecting privacy in a volatile environment.

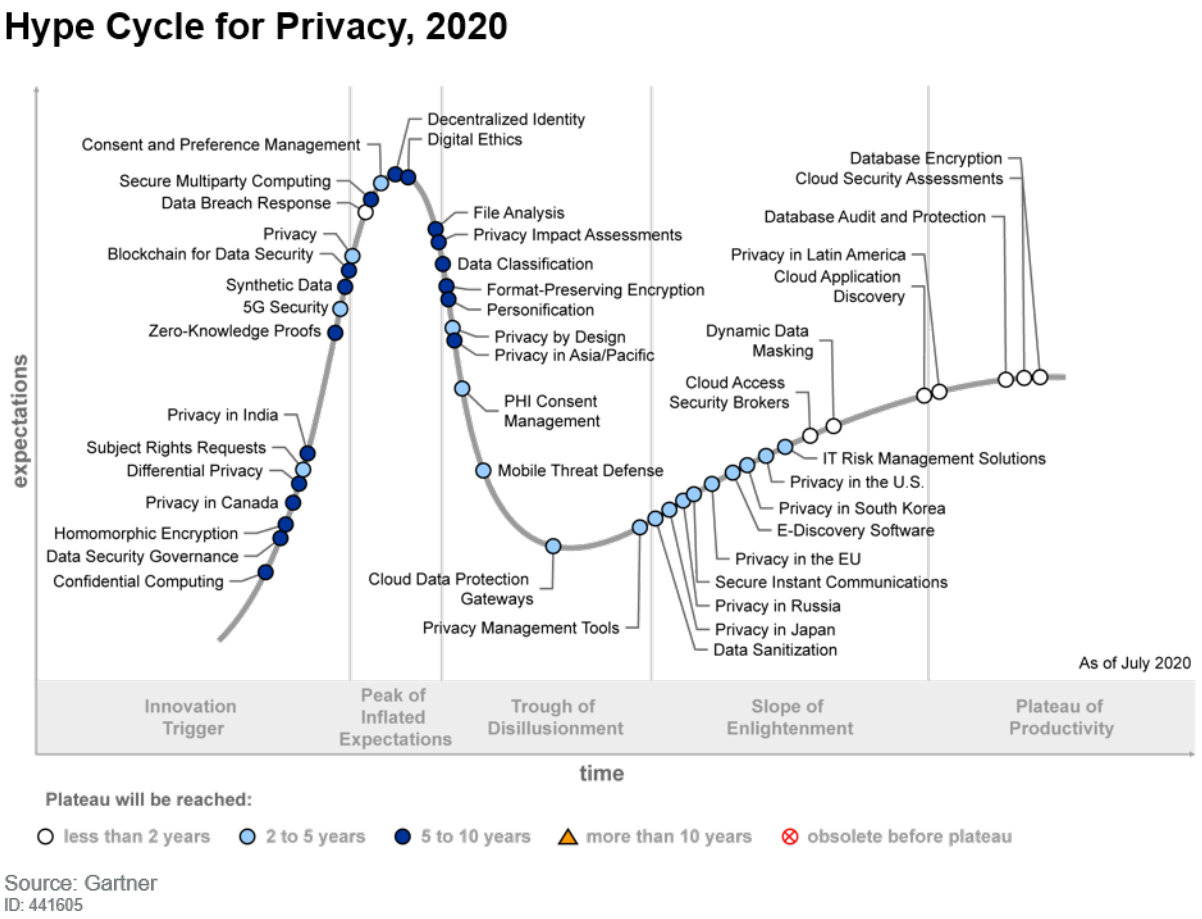
The Hype Cycle

This Hype Cycle deals with international regulatory developments, as well as the technologies that help protect personal data. Privacy laws, after all, follow a Hype Cycle of their own. Initially, regulations may lack detailed guidance, case law is still missing, and there is confusion around the exact requirements and upcoming enforcement. Around the peak, when political pressure is greatest, a legislative body passes new laws. An initial lack of enforcement often leads into the Trough of Disillusionment. After a time, enterprises gain experience, and regulators set enforcement precedents and publish advisories. Vendors improve compliance support, and eventually privacy is considered a standard of default due care. At this point, the law has reached the Plateau of Productivity.

Within the organization, a “privacy mature” environment can only be created by using a combination of privacy management, privacy control and security capabilities integrated with personal data-processing activities. Cutting across various disciplines, privacy is much more than a security or technology discipline; SRM leaders must maintain a working relationship with all business units to actively promote coordinated action toward compliance. This enables them to understand the relevance of tools to context and ensure that the right tool is in the right place. For example, opportunities can be found in business process reengineering, which is neither a security, nor an IT-specific discipline. Similarly, the application of data minimization to the data life cycle is more a discipline than a technology.

Beyond sanctions, privacy risk mitigation focuses primarily on postbreach financial risks, consumer trust decay and brand damage. The technologies highlighted in this Hype Cycle enable or enhance control over personal data use (e.g., discovery and data classification), create transparency and demonstrate compliance (privacy management tools), and treat the risk of data misuse (e.g., differential privacy and homomorphic encryption). They also mitigate the impact of unintended consequences (format-preserving encryption).

Figure 1. Hype Cycle for Privacy, 2020



Source: Gartner
ID: 441605

The Priority Matrix

The type and benefit of technological aid vary widely. Rather than leading operations, the application of technology should follow gap and risk assessments in a supporting role. Treating privacy risk means focusing on the individual (data subject); thus, benefits depend on the types of threats prevented and the types of business activities enabled. For example, data classification and file analysis are not only applied to personal data, but also benefit generic business risk treatment. On the other hand, Privacy by Design represents a cultural change to the processing of personal data, and its impact is not easily quantified.

Proactive risk reduction can be achieved through competent data access governance and pseudonymization techniques, such as encryption, masking and tokenization. Customer trust levels can be enhanced with a positive privacy UX, including the management of subject rights requests. Evolving technologies include secure multiparty computing (SMPC), and analytics activities benefit from privacy preservation through differential privacy or homomorphic encryption. Compliance demonstration, on the other hand, is aided by purpose-built privacy management tools. New

business and IT contexts, such as the development of 5G networking, mean that SRM leaders and vendors need to keep evolving to meet new privacy threats. Acknowledging the need for both privacy and business benefits, new technologies surface as vendors improve the offerings and broaden combinations of capabilities.

Figure 2. Priority Matrix for Privacy, 2020

Priority Matrix for Privacy, 2020

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational		**Subject Rights Requests**	**Data Security Governance** **Homomorphic Encryption** **Secure Multiparty Computing**	
high	**Cloud Access Security Brokers** **Cloud Security Assessments** **Data Breach Response** **Database Audit and Protection**	**E-Discovery Software** **IT Risk Management Solutions** **Privacy** **Privacy in South Korea** **Privacy in the EU** **Privacy in the U.S.** **Privacy Management Tools**	Blockchain for Data Security Data Classification Decentralized Identity Differential Privacy Digital Ethics Personification Privacy Impact Assessments Privacy in Asia/Pacific Synthetic Data	
moderate	**Cloud Application Discovery** **Database Encryption** **Dynamic Data Masking** **Privacy in Latin America**	5G Security Cloud Data Protection Gateways Consent and Preference Management Data Sanitization Mobile Threat Defense PHI Consent Management Privacy by Design Privacy in Japan Privacy in Russia Secure Instant Communications	Confidential Computing File Analysis Format-Preserving Encryption Privacy in Canada Privacy in India Zero-Knowledge Proofs	
low				

As of July 2020

Source: Gartner
ID: 441605

Off the Hype Cycle

The following changes have been made to this year's Hype Cycle:

- Homomorphic encryption, differential privacy, subject rights requests, 5G security and synthetic data were added at the onset of the Hype Cycle.
- Subject rights requests and 5G security have wide applicability (5% to 20% of the target audience), due to:
  - The enshrinement of individual rights in the majority of privacy regulations
  - The number of nations actively building out 5G networks
- Privacy-enhanced multiparty computing is being applied in wider use cases, and has been renamed SMPC.
- For naming convention consistency:
  - The European Union (EU) Generation Data Protection Regulation (GDPR) has been renamed privacy in the EU
  - U.S. privacy laws has been renamed privacy in the U.S.
  - Privacy in South America has been renamed privacy in Latin America
- Test data management is being replaced by numerous other data treatment techniques. Thus, it has reached the Plateau of Productivity and fallen off the Hype Cycle this year.

On the Rise

Confidential Computing

Analysis By: Steve Riley

Definition: Confidential computing is a security mechanism that executes code in a hardware-based trusted execution environment (TEE), also called an enclave. Enclaves isolate and protect code and data from the host system (plus the host system's owners), and may also provide code integrity and attestation.

Position and Adoption Speed Justification: In most cases, confidential computing implementations make use of Intel's Software Guard eXtensions (SGX) or ARM TrustZone. This architecture and set of instructions allows developers to isolate and execute code in private regions of memory unavailable to any process outside those regions, including processes at higher privilege levels. To take advantage of these enclaves, developers must specifically code for them (unless they add a software intermediary). AMD offers a similar technology called Secure Encrypted Virtualization (SEV); however, it doesn't shield code from the platform owner and doesn't offer integrity protection.

Although confidential computing can be deployed on-premises, it is in the context of public cloud that most organizations express interest. Inquiry trends reveal increased anxiety among cloud-using organizations about CSP staff eavesdropping into or tampering with customer workloads. Confidential computing is an emerging mechanism that CSPs could offer their customers to alleviate these concerns. In a cloud provider's implementation, it would rely on a combination of hardware and software that attempts to prevent provider and unapproved third-party access to data in use.

However, the major cloud providers aren't rapidly adopting SGX or making it broadly available. Microsoft Azure offers one type of SGX instance in some regions, IBM offers SGX instances in Cloud Kubernetes Service bare metal hosts in most regions, and Alibaba supports SGX on bare-metal instances only. Intel's apparent lack of urgency at making SGX available in data center-class Xeon processors exacerbates the situation. Google has yet to announce its form of confidential computing. Amazon Web Services follows a different path: AWS Nitro Enclaves creates a separate instance that contains a single encrypted communications path to a parent instance and is hardware-isolated such that the parent instance has no access to the enclave's memory or compute. Gartner surmises that CSPs are reluctant to cede any part of their infrastructure to opaque elements over which they have little to no control.

Various emerging abstraction layers can eliminate the requirement for developers to code explicitly for a particular CPU's TEE. Asylo (by Google) and Open Enclave (by Microsoft) are available now. Carrying the abstraction layer notion even further, Fortanix Runtime Encryption removes the need to modify code, allowing existing applications to take advantage of enclaves. The Confidential Computing Consortium, a Linux Foundation project, aims to organize these efforts without imposing strict standards.

User Advice:

- Confidential computing isn't plug-and-play, and should be reserved for the highest-risk use cases. It represents a high level of effort, but offers diminishing marginal security improvement over more pedestrian controls like TLS, MFA, and customer-controlled key management services.
- Allocate time in the calendars of cloud application developers and cloud security architects to learn about the available confidential computing options and to experiment with the technology. Not all TEEs offer the same security guarantees or the same requirements for integration with existing and new code. In addition, confidential computing doesn't protect from vulnerable application code, and may contain its own exploitable vulnerabilities.
- Design (or duplicate) a sample application using one of the available abstraction mechanisms and deploy it into an instance with an enclave. Perform processing on datasets that represent the kinds and amounts of sensitive information you expect in real production workloads to determine whether confidential computing affects application performance, and to seek ways to minimize negative results.
- Review alternatives that achieve similar protection of sensitive data in use, such as multiparty encryption, data masking or tokenization. None of these require specific hardware.

- Examine confidential computing for projects in which multiple parties, who might not necessarily trust each other, need to process (but not access) sensitive data in a way that all parties benefit from the common results. None of the parties should control the TEE in this scenario.

Business Impact: Confidential computing potentially removes the remaining barrier to cloud adoption for highly regulated businesses or any organization concerned about unauthorized third-party access to data in use in the public cloud. It's likely that auditors and regulators will demand, for certain data types, increased protection including high barriers to provider and government access. Confidential computing can provide such protection now. Be mindful of the potential performance impacts and the extra cost. IaaS confidential computing instances (whether SGX-based or otherwise) will cost more to run.

Confidential computing is a marginally useful but technically challenging mechanism appropriate only for the most sensitive of use cases. Protecting data in use shifts trust to the CPU's ability to enforce enclave boundaries. However, hardware may not always be trustworthy, as the Spectre and Meltdown vulnerabilities demonstrated. Speculative execution is exhibiting many unexpected side effects, and could be used to conduct side-channel attacks that reveal SGX-protected secrets. Furthermore, SGX (and other TEEs) are themselves interesting to attackers and are likely to attract their attention.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Alibaba Cloud; Fortanix; IBM Cloud; Intel; Microsoft Azure; Private Machines

Recommended Reading:

"Achieving Data Security Through Privacy-Enhanced Computation Techniques"

"Solution Criteria for Cloud Integrated IaaS and PaaS"

"Securing the Data and Advanced Analytics Pipeline"

"How to Retain the Right Kinds of Control in the Cloud"

"How to Make Cloud More Secure Than Your Own Data Center"

Data Security Governance

Analysis By: Brian Lowans; Bart Willemsen

Definition: The data security governance (DSG) framework enables the assessment, prioritization and treatment of business risks caused by security, data residency, privacy and other incidents that affect data.

Position and Adoption Speed Justification: The DSG framework offers a balanced approach to define how practical data protection can be implemented through data security and privacy controls. Each dataset has a different business purpose, and different business and security risks. DSG requires cross-collaboration among CISOs, CDOs and business leaders to break down barriers of independent governance processes. The rapid emergence of data protection and privacy regulations also requires collaboration with the data protection officer (DPO) to ensure that adequate privacy impact assessments are integrated through DSG.

User Advice: The DSG framework is constructed to manage security policies across a portfolio of datasets. The flow and analytics applied to each dataset will create policy decisions based on privacy, confidentiality, integrity, availability, purpose and lifetime issues. However, organizations typically need to deploy dozens of security products. However, each product is siloed, due to the security functionality, the controls it offers and/or the data storage on which it operates. No single security product or control will mitigate a business risk sufficiently. Therefore, DSG is critical to assess how security policies can be orchestrated through the various product controls, and to identify and minimize gaps or inconsistencies in how these controls are applied. These gaps and inconsistencies create the need to develop a continuous data risk assessment (DRA). The DRA forms the basis for assessment and creation of security policies that are required under DSG. These policies are based on three basic principles:

- **Data —** Each dataset has business purposes and risks that need to be governed.
- **User Account —** Each user account will be granted a variety of roles and affiliations to project teams, devices and IT. User accounts are also being provisioned for access by programmable devices and artificial intelligence (AI).
- **Access —** A variety of products provision access, privileges and entitlements that are encompassed by data security, identity access management (IAM), and applications or analytics.

Orchestration of policies by DSG across the variety of data security, IAM and application management consoles is a complex process. There are some core principles that help:

- Identify and map all data storage and processing silos on-premises and in cloud services.
- Identify all products that manage access to, or security of, data.
- Identify the data discovery and classification products deployed, and their ability to cover unstructured and structured data.
- Identify which datasets and volumes are stored in each silo.
- Identify which datasets are encompassed by each security console.
- Map which users and privileges are granted by each console.
- Identify inconsistencies or gaps in each user's access to datasets.
- Identify potential roadmaps to synchronize and orchestrate more-consistent policies.

- Identify the gaps and risks created by the existing product portfolio that cannot be addressed by orchestration and recommend changes.

The business risk analysis process can then evaluate the impacts of specific monetization options and innovations, using infonomics to estimate profitability in terms of financial assets and liabilities. Prioritization of these opportunities can then be established using principles, such as Gartner's financial data risk assessment (FinDRA). Any broader data and analytics governance effort needs to align to DSG, because the two approaches look at applying policies to the same piece of data, possibly in the same time and space. Therefore, cooperation and collaboration between the CDO and the CISO are essential to reduce redundancy and waste.

Business Impact: Organizations focused on digital business strategies are seizing opportunities for growth by creating value from the increasing velocity, volume and variety of datasets. However, they face huge challenges to treat the growth of associated business risks arising from security and compliance issues. Additional security, privacy, trust and life cycle control issues grow, as data is shared with partners and ecosystems. Gartner's DSG framework enables the assessment and prioritization of business risks and allows organizations to establish a defensible data security strategy.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Recommended Reading:

"Use the Data Security Governance Framework to Balance Business Needs and Risks"

"Use Infonomics to Quantify Data Monetization Risks and Establish a Data Security Budget"

"Develop a Financial Risk Assessment for Data Using Infonomics"

Homomorphic Encryption

Analysis By: Mark Horvath; Mark Driver

Definition: Homomorphic encryption (HE) is algorithms that enable computation on encrypted data. Fully homomorphic encryption (FHE) supports arbitrary operations, but has significant performance impact and is not yet practical. Partial homomorphic encryption (PHE) supports more limited subsets of operations with lower performance impact than FHE, but also more limited use cases. Currently, commercial products are supported by some version of PHE.

Position and Adoption Speed Justification: Although PHE offers some extremely compelling use cases for privacy, IP protection and encrypted computation, it's a technology still in a very early phase without much support from standards, testing and large-scale use cases. Every vendor has a proprietary take on the technology, and, as it begins to mature, products and technology can easily change very quickly. Recent innovations have allowed PHE to start to be included in commercial

products, although user implementations are all in a proof-of-concept phase. While there is still significant work to do in both speeding up PHE, limited specific uses, like encrypted search or multiparty computing, have come onto the market and are seeing some experimental adoption.

User Advice: Gartner advises organizations considering adopting homomorphic encryption products to:

- Brainstorm with your technical and executive teams about the opportunities within your specific products and services. For example, come up with a list of five to 10 use cases for HE to improve customer adoption and remove barriers to adoption of core solutions.
- Treat potential HE projects as experiments, keeping in mind the early stage of the technology as a whole and the significant not-real-time nature of the products. Consider these experiments as proofs of concept until the technology matures.
- Continue existing security controls. PHE does not necessarily negate the need for other security controls, such as protecting decrypted text while in-memory, data residency requirements and access control.
- Assess the core benefits of using homomorphic encryption combined with quantum-safe and privacy-preserving computation techniques.

Leverage opportunities for encrypted data in use by integrating homomorphic encryption into encryption, messaging and third-party data analytics services, which must consider the implications of using homomorphic encryption in their solutions to leverage opportunities for encrypted data in use.

Business Impact: Product managers responsible for one or more IT solutions that share data with third-party suppliers or consumers should ask their product teams, “How might HE impact your product strategy over the next five years?” “How might HE simplify or streamline existing business practices?” “Would HE support remove trepidation or concern among potential customers for your products/services?” For example, if you are a cloud-based SaaS platform provider, would HE help reduce client concerns and lower adoption inhibitors?

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Duality Technologies; Enveil; IBM; Inpher; IXUP; Microsoft

Recommended Reading:

“Emerging Technologies: Homomorphic Encryption for Data Sharing With Privacy”

“Emerging Technologies and Trends Impact Radar: Security”

“Achieving Data Security Through Privacy-Enhanced Computation Techniques”

Privacy in Canada

Analysis By: Bernard Woo; Bart Willemsen

Definition: At the country level, privacy in Canada is regulated for commercial organizations by the *Personal Information Protection and Electronic Documents Act* (PIPEDA, effective 2001) and the law known as the "Canada's Anti-Spam Legislation" (CASL, effective 2014). There are privacy laws at the provincial level, although the majority of those are sector-specific (e.g., health). Canada is one of the nations that has an "adequacy status" with the EU and will have this standing reviewed under the GDPR in the next two years.

Position and Adoption Speed Justification: First steps toward reforming PIPEDA have been taken. Proposals include a focus on enhancing individual control, enabling responsible innovation and enhancing oversight and enforcement. The reform is identified as a priority by government.

The federal regulator conducted a review of its position on cross-border data transfers under PIPEDA. No change to the existing position is considered necessary, even though current protections in PIPEDA are increasingly deemed insufficient. Instead, the regulator now focuses its efforts on strengthening protections for cross-border data transfers in a reformed law.

Another area where PIPEDA requires reform would be with respect to the use of AI. Public feedback is sourced as to where PIPEDA requires strengthening specific to innovations in ML and AI. Further refinement of the overall scope of legislation is expected to continue alignment with EU privacy legislation.

As for enforcement, there are incidental occurrences at best. One current example relates to legal proceedings against Facebook in federal court, following a joint regulatory investigation of a complaint about Facebook's practices regarding third-party processing of personal data.

User Advice:

- Security and risk management (SRM) leaders in organizations that have been processing EU resident personal data in Canada will need to pay attention to developments with respect to the country's adequacy status. Should Canada lose its adequacy status with the EU, organizations will need to establish an alternative mechanism to transfer and process this data in Canada, such as standard contractual clauses.
- SRM leaders in organizations operating in Canada should monitor PIPEDA reforms for impact to operations. Based on current proposals, it is likely reforms will lead PIPEDA closer to the model provided by the GDPR. SRM leaders can therefore look to practices demanded by the GDPR for guidance on how existing operations can be strengthened.
- SRM leaders in the health sector need to monitor sector-specific laws such as the *Personal Health Information Protection Act* (PHIPA) in the province of Ontario.
- SRM leaders must consider that regulators in Canada are increasing their enforcement activities. SRM leaders therefore need to drive the completion of privacy impact assessments

when there are changes in the processing of personal data. This will identify potential privacy-related risks and require appropriate mitigating actions be taken.

- SRM leaders in organizations that send "commercial electronic messages" (CEMs; e.g., marketing emails) to recipients in Canada are reminded that CASL carries fine up to $10,000 (CAD) per violation. SRM leaders in such organizations will do well to regularly review the consent on file and the contents included with each CEM against the requirements imposed by CASL.

Business Impact: Canada has seen a fairly stable status quo from a privacy perspective for the last decade. However, the country is expected to see substantial change over the coming one to three years which will cause significant disruption to operations due to shifts in the regulatory landscape.

PIPEDA reform will continue, and the extent of changes will have to become clear with time. Based on proposals outlined thus far, it is anticipated that individual rights will be expanded (e.g., to include the right to data portability), language will be introduced with respect to the use of deidentified (anonymized, pseudonymized) data, as well as increased enforcement capabilities for the regulator. As such, appropriate attention for the privacy UX will be required.

Organizations that prepare to adhere today to more stringent requirements in advance will see long-term benefits of cost spreading, client retention and trust enhancements, and a less disrupted international trade opportunity. This is to be flanked and complemented by appropriate attention for the privacy UX.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Recommended Reading:

"Market Guide for Subject Rights Request Automation"

"Privacy as a Partner: Privacy as a Partner: Building Citizen Trust in Public-Private Partnerships"

"Toolkit: Assess Your Personal Data Processing Activities"

"Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

Differential Privacy

Analysis By: Van Baker

Definition: Differential privacy is a system for sharing information about a dataset while withholding or distorting certain information elements about individuals in the dataset. The system uses an exact mathematical algorithm that randomly inserts noise into the data and ensures that the resulting analysis of the data does not significantly change whether the individual's data is included or not.

Position and Adoption Speed Justification: As sensitive electronic data is stored, inadvertent exposure of personal data via analytics is a risk. Additionally, hackers may gain access to more databases holding individual information that is potentially damaging if revealed or used against them. This increasingly puts enterprises at risk of legal liability if they don't protect this data. One defense against this is the use of differential privacy systems. This effectively delivers the same analytic results whether individual's data is included in the dataset or not. Differential privacy systems use probabilistic randomization of the data elements in the dataset to make it impossible for malicious actors to reverse engineer those data attributes and tie them to a specific individual. While not specifically designed to prevent reidentification attacks, differential privacy does effectively protect against these attacks. Differential privacy does have a weakness if the algorithm is repeatedly applied to the data.

User Advice: Differential privacy systems should be employed when datasets have significant value to be extracted but the information contains sensitive individual information or legally protected information. It can be applied to any information that is associated with personally identifiable attributes or is defined as sensitive information under a data protection regulation. The increasing sophistication of attacks against data repositories will make the use of differential privacy systems and other methods such as data encryption increasingly necessary for organizations holding personally identifiable information. Organizations looking to monetize their data assets containing personally identifiable information will find themselves under increasing scrutiny. A failure to employ differential privacy and other data protection mechanisms will likely increase the organizations' exposure to legal proceedings and potentially damaging financial penalties.

- Enterprises holding sensitive data assets with personally identifiable information should explore the use of differential privacy systems to decrease the likelihood they will expose sensitive data that can be tied to individuals.
- Enterprises should also take other measures to protect data assets containing sensitive data that contains personally identifiable information.
- Organizations should not assume that differential privacy systems alone are enough to prevent breach of sensitive information.
- Enterprises operating in high-performance environments and also requiring a high-level of precision in their models are encouraged to compare this approach with other privacy preserving compute platforms.
- Differential privacy can be applied at the data level or the group level and should be deployed appropriately.
- Differential privacy can be used in isolation but is best used with other methodologies to best protect individual information and the enterprise.

Business Impact: Businesses increasingly recognize the value in data such as customer information in CRM databases however they also find themselves liable for protection of this sensitive personal data. Regulations that define how enterprises may use this information are increasingly being defined and implemented and the liability for leaking such information can be substantial. In addition, the reputation of the business and the trust associated with the business

can be significantly damaged by breaches of sensitive information. This will require businesses to use whatever means available to protect datasets containing sensitive information. This exposure is not limited to the datasets in control of the business as malicious actors can increasingly combine data sources to reidentify individuals even if the data used by the business is anonymized. As such, businesses should employ whatever means available to protect personally identifiable information from being exposed.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: 01Booster; Hazy; LeapYear

Recommended Reading:

"Boost Your Training Data for Better Machine Learning"

Subject Rights Requests

Analysis By: Nader Henein

Definition: Subject rights requests (SRRs) are rights that empower individuals to make requests regarding their data, and organizations handling this data must address these requests in a defined time frame.

These rights come in three categories, informative, corrective and restrictive. Their execution implicitly requires multiple capabilities of a modern privacy management program such as personal data discovery and mapping. Best practices dictate that request fulfillment follow a repeatable and scalable process for compliance and efficiency.

Position and Adoption Speed Justification: SRR management has evolved from near anonymity to center-stage status in a short two-year span due to the advancement in privacy legislation (such as the GDPR, CCPA and LGPD) and increased consumer concern over the handling of their personal data. Today, over 1 billion individuals accounting for almost one-third of the global economy can exercise these rights freely.

The SRR market is composed of an ecosystem of vendors that provide capabilities to support the stages involved in SRR fulfillment. These capabilities serve organizations in any number of areas to deliver partial or full process automation from capture to response.

User Advice: Privacy is personal. How organizations handle the personal data of their customers and their families will either garner loyalty or, at the other extreme, litigation. Consumers today are increasingly inclined to switch to the competition, and in some cases pay a premium, if that is where they believe their personal data will be best handled.

To nurture customer loyalty and support regulatory compliance, SRM leaders must deliver a user-centric experience for SRR fulfillment built on transparency and clear communication.

The process should start by establishing the foundational metrics around subject rights requests:

- **Time:** The amount of time it takes to respond to a single request.
- **Cost:** The cost of a request is often calculated based on the person-hour rate of the team processing SRRs as well as any other resources involved.
- **Scale:** The scale denotes the number of requests an organization can fulfill in the requisite time frame, a period often defined by applicable laws.

These metrics will allow SRM leaders to propose a level of automation in SRR fulfillment in line with the projected outlay.

Business Impact: The business impact of not complying with SRRs is twofold:

- Fines levied by regulators for failure to comply; these rulings will mandate executing the request without delay.
- Erosion of the trust relationship between the organization and its customers. The loss of trust may also escalate in more destructive requests such as deletion (commonly known as the right to be forgotten) or limitation of processing.

On the other hand, taking a proactive approach to transparency through privacy portals allows individuals to self-serve subject rights. Through automation, SRM leaders can support cost optimization efforts and build a stronger foundation of trust with consumers.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: BigID; Exterro; OneTrust; SECURITI.ai; TrustArc; WireWheel

Recommended Reading:

“Market Guide for Subject Rights Request Automation”

“How to Prepare for the CCPA and Navigate Consumer Privacy Rights”

Privacy in India

Analysis By: Bart Willemsen; Bernard Woo

Definition: Privacy in India got a boost with a 2017 Supreme Court ruling affirming the right to privacy as a fundamental right in the Constitution. Currently, privacy principles are guided by Information Technology Act (ITA) of 2000 and Information Technology (“Reasonable security

practices and procedures and sensitive personal data or information") Rules, 2011 (Rules). The Personal Data Protection Bill (PDPB) as amended 2019, flanked by an elaborate privacy framework, brings over 1 billion people closer to GDPR-like protection.

Position and Adoption Speed Justification: Initiatives like "Digital India" and the country's biometric-based identity system Aadhaar have fueled the need for enhanced control over personal data processing. Aadhaar's use has permeated across many aspects of day-to-day life. Data breaches and news coverage of compromise within the database has made citizens wary. The Supreme Court of India has formally limited the use of Aadhaar only for welfare payments or filing of tax returns, but alternative usage persists. Formal enactment of the PDPB suffers delay and enactment follows in 2020 or 2021.

For now, India's data protection standards are found in the ITA and Rules, aside from requirements regarding for example data residency in industry verticals (e.g., finance and insurance). These fragmented privacy rights obligate corporations to take steps toward protecting consumer privacy. But overall coverage of privacy is weak, and organizations often are not directly impacted. However, given the position of India's IT industry globally, compliance with regulatory and contractual requirements from global clients and partners continues to be a catalyst for change. As public demand for consistent privacy protection has only begun recently, it will take time for the overall privacy culture and laws to mature.

User Advice: Security and risk management (SRM) leaders must take into consideration the existing requirements from the ITA (2000), Rules (2011), residency requirements imposed by the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority (IRDA) and the proposed data protection requirements in the PDPB altogether. Many of the foundational principle-based elements in the PDPB resemble those found in the EU's GDPR and establishing a mature privacy program that is prepared for the PDPB alone takes two years. SRM leaders should focus on these principles primarily, including purposeful processing, the position of a privacy impact assessment, "adequate" security, the facilitation of elaborate privacy rights for individuals, and principles of Privacy by Design, transparency, notice and consent.

Implement an overarching privacy framework rather than having to deal with each compliance requirement in silo. Draft and implement organizationwide privacy policies in line with best practices. In the absence of a dedicated privacy law, organization-level privacy policies will enhance customer trust, reduce the data footprint and accompanying storage costs, and similarly reduce financial and brand damage when incidents are both prevented and, should they occur, handled maturely and responsibly.

Business Impact: With the rise in number of and adoption of data localization requirements, the impact on businesses have started becoming prominent which ranges from implementing data mirroring to establishing infrastructure in India. The 2019 final draft published contains specifications on both "critical data" and "sensitive data."

- Financial details are (also) defined as "sensitive data," in addition to other information. Sensitive data is primarily to be processed within India only. Transfers are allowed only in specific instances and a copy must always remain in India.

- What is defined as “critical data” is yet to be clarified. “Critical data” must be processed solely within the country.

In addition, organizations face various regional and industry-specific requirements, depending on where they operate. Organizations must enhance transparency on purposeful processing, and provide GDPR-like privacy rights to individuals. Global entities operating in India will also have to comply with regulatory requirements; for example, organizations processing payment information have to comply to the data localization requirements laid down by RBI.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Recommended Reading:

“Toolkit: Assess Your Personal Data Processing Activities”

“Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria”

Zero-Knowledge Proofs

Analysis By: David Mahdi

Definition: Zero-knowledge proofs (ZKP) are privacy-preserving messaging protocols that enable entities to prove that information available to both of them is correct, without the requirement to transmit or share the underlying information. Blockchain platforms have been evolving to include this privacy-oriented mechanism.

Position and Adoption Speed Justification: MIT first developed the concept of ZKP in the 1980s. In particular, the challenge was to overcome the possibility of fraudulent representation of information. Rather than just focusing on an entity (prover) who tries to persuade the receiver (verifier) that the information is accurate (either false or true), the goal is to also address the issue of a verifier learning more about the information than merely if it is accurate or not. This challenge has applicability in a wide range of use cases especially in the context of authentication and transaction verification. Other cases include payments, custody management, AML/KYC, consumer IAM, medical records, mergers and acquisitions, etc.

To operate effectively, ZKP must have completeness (of process), soundness (of information), and zero knowledge (of anything other than the proof). This challenge is highly relevant to blockchains and distributed ledgers as a core tenet of their operation is data sharing. The zero-knowledge approach is used by blockchain platforms and cryptocurrencies in the form of zk-SNARKs, which are better-suited to a blockchain context due to greater efficiency and reduced need for interactivity. Hawk is an application of ZKP to smart contract domain, where the state of the computation is encrypted. An enabling cryptographic construct for ZKP is homomorphic encryption, which allows

for computation on encrypted variables without revealing their values. Zcash (and its predecessor, Zerocash) is an early example of applying ZKP as an extension to the Bitcoin Protocol.

In July 2016, Ethereum developers (such as Vitalik Buterin, the founder of Ethereum) worked in combination with ZKP experts to add a lightweight implementation of zk-SNARKs to the Ethereum platform, called ZoE. It is likely that future versions of Ethereum will incorporate a more robust ZKP capability. Major platforms that seek to compete with Ethereum and Bitcoin will add ZKP capability as well, and its value as a point of differentiation in a crowded competitive platform landscape will diminish. Overall, ZKPs are privacy-preserving messaging protocols that enable entities to prove that information available to both of them is correct, without the requirement to transmit or share the underlying information. Leveraging ZKPs limits the requirement for mass decryption and encryption of all the data elements, which has benefits for the efficiency of the network as well as the potential adoption of blockchain/distributed ledger technology. Ultimately, by leveraging ZKPs, service providers, and others can reduce their reliance on honeypots of user data, to help mitigate against mass data breaches.

A challenge is that variety of methodologies and the multiplicity of types of ledgers and approaches to data management inhibits adoption. Moreover, ZKP will need to scale at the rate of DL transactional volumes in order to be effective, and this is yet to be proven.

User Advice:

- Work with security and risk management leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Understand how ZKP can benefit use cases that require privacy protection, but be realistic with the current immaturity of ZKP solutions and approaches.
- Evaluate how such controls may impact transaction authentication and ultimately consumers.
- Assess the impact on the broader information management strategy.
- Assess the architectural implications for using ZKP with different blockchains and distributed ledgers.

Business Impact: Most blockchain platforms today offer a number of core benefits, but namely, those of integrity and availability. Although this may benefit a number of approaches to ensure transaction and data security, confidentiality was not covered by the core of blockchain platforms. With the addition of ZKPs to blockchain platforms, security and risk management leaders now have the potential to cover information security use cases that require confidentiality, integrity and availability (CIA). Extending CIA, this also provides privacy focused security leaders with alternatives regarding privacy protection, and sensitive data minimization. Ultimately, business impact can be significant in terms of institutions and individuals being able to better protect and prove the context and details of information while simultaneously being able to maintain confidentiality. This would also limit the requirement for mass decryption and encryption of all the data elements, which has benefits for the efficiency of the network as well as the potential adoption of blockchain/distributed ledger technology.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Ethereum; Evernym; IBM; Zcash

Recommended Reading:

"Market Guide for Blockchain Platforms"

"A Technical Primer for Assessing a Blockchain Platform"

"Innovation Insight for Blockchain Security"

"Cool Vendors in Blockchain Technology"

"Predicts 2019: The Ambiguous Future of Privacy"

"Cool Vendors in Privacy Management"

5G Security

Analysis By: Sylvain Fabre; Bernard Woo

Definition: 5G security is enabled by a set of 5G network mechanisms, and improves 4G security with:

- Unified authentication (4G authentication is access dependent).
- Flexible security policy for diverse use cases (versus single 4G policy).
- Encrypted transmission Subscription Permanent Identifier (SUPI) prevents International Mobile Subscriber Identity (IMSI) leakage for user privacy.

Position and Adoption Speed Justification: 5G security is not a priority in many deployments; standards won't cover everything — implementation will hugely influence outcomes (e.g., private network versus public infrastructure). Switching on security features is up to the CSPs.

- 5G will increase number and diversity of connected objects, potential DDoS attack vectors and entry points; this also provides more telemetry for anomaly detection.
- More 5G private, dedicated networks will be deployed by enterprises (more security conscious than consumers).
- Legacy networks and devices will interconnect with 5G.
- 5G infrastructure virtualization, automation and orchestration of a service-based architecture increases exposure.

- Slicing virtual networks across shared infrastructure impacts security due to lateral movement risk, and cross-slice permeability issues.
- Wider ecosystem delivering industrial 5G use cases, with varying security competencies and credentials, make SLAs, service assurance including E2E security, challenging.
- Backward compatibility with 4G/Long Term Evolution (LTE) means some legacy security issues persist in 5G.

User Advice: Don't rely exceedingly on network 5G security, end users will still have to continue using VPNs and identity management.

In addition, security leaders leveraging 5G, including for industries, should:

- Anticipate increased attack risk such as DDoS by improving equipment and software design of 5G network infrastructure and endpoints, and recovery procedures.
- Implement layered-DDoS defense with best of cloud scrubbing center, cloud web application firewall, bot mitigation, DNS protection, ISP and on-premises DDoS appliances. Determine effectiveness of protections from incremental add-on solutions an ISP or CDN can sell.
- Evaluate DDoS protection services from current CSP or cloud providers as a possible failover for key applications when on-premises DC is under attack.
- Initiate effective mitigation by correlating network traffic, application availability and server performance. Outages may be due to human or system error rather than attacks.
- Consider interoperability with other networks (e.g., authentication of Wi-Fi devices). Ensure 5G device hardening to reduce possibility of being used as botnets.
- Segment IoT devices with different incident responses.
- Complement 5G infrastructure security with distributed anomaly detection/monitoring including edge and core slicing.
- Decide any trade-offs between secrecy, capacity, delay, quality of service (QoS), compute and energy efficiency by use case.
- Implement edge protection concepts used in application security for elasticity and focused on app-layer protection, and commonly provided via a CDN provider, SaaS or cloud provider.

Security for 5G systems encompasses need to include in network deployments:

- Cross-network layer security (e.g., between 5G macro and small cell layers)
- E2E security (e.g., managing strength of different algorithms, generating and negotiating secret keys, confidentiality protection)
- Cross-CSP 5G network domain security (e.g., in R16, several cloud service providers [CSPs] could provide slices for a given 5G service)
- Leverage user traffic integrity protection which is available now

Traffic interception may require formal and time-sensitive reporting to clients due to maturing data protection regulations.

Implement patching policies and procedures on devices used for network configuration given 5G's reliance on software.

All 5G network infrastructure vendors implement the same 3GPP standards for 5G security; however development processes may vary; concerns about specific vendors as well as geopolitical tensions have increased procurement scrutiny around 5G infrastructure.

5G network infrastructure requires more antennas, promoting sharing with different CSPs or utility providers, or multitenant scenarios. It needs the review and update of hardware protection protocols, including physical measures to address recent increases in vandalism based on fake news.

Embed privacy-protective features into endpoint/IoT devices to manage potential privacy risks.

Plan for lower security context anytime your 5G devices connect to a legacy 3G or 4G network.

Business Impact: Increased controls could impact QoS, increase latency and lower data rate due to traffic encryption overhead.

Guaranteed security levels may enable 5G use in more demanding use cases, using other improvements, like:

- Home control feature enables network to verify device location when the device is in a visited network, preventing spoofing attacks on device locations involving false signaling messages to request device identifier and location, and then intercept ongoing communications.
- 5G mitigation against bidding down attacks prevents a fake base station from making UEs believe that the BTS ("IMSI catcher") does not support a specific security feature and use a previous mobile network technology.
- Flexible security policies and other chargeable features such as slice as a service, QoS SLAs for latency etc. in 5G allow premium pricing.
- 5G security adds value for CSPs but may be adding complexity for business users.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Ericsson; Huawei; Intel; Mobileum; Netcracker; Nokia; VIAVI Solutions

Recommended Reading:

“Market Trends: Strategies Communications Service Providers Can Use to Address Key 5G Security Challenges”

“Reduce Privacy Risks When Using 5G Products and Services”

“Market Guide for Mobile Threat Defense”

“Protecting Web Applications and APIs From Exploits and Abuse”

Synthetic Data

Analysis By: Anthony Mullen; Alexander Linden

Definition: Synthetic data is a class of data that is artificially generated, i.e., not obtained from direct measurements. Generation can use different methods such as statistically rigorous sampling from real data, semantic approaches, generative adversarial networks or by creating simulation scenarios where models and processes interact to create completely new datasets of events.

Position and Adoption Speed Justification: One of the major problems with AI development today is the burden in obtaining real-world data and labeling it so that AI may be trained effectively. For example, retail environments contain endless combinations of product, store layout and observable shopper behavior — a challenge for computer vision training. Also, autonomous vehicles require millions of hours of training data. Synthetic data addresses the problem of volume and variety for sparse, nonexistent or difficult to get data. There are three primary methods we see in the marketplace today:

- Sampling to generate data according to some distribution
- Generative adversarial network (GAN) architectures that mimic real data
- Agent-based techniques in simulations

Synthetic data, today at least, is not a panacea — it can have bias problems, miss natural anomalies, be complicated to develop or may not contribute any new information to the existing real-world data. Data quality is tied to the model that developed it. Yet, Gartner believes, the pros outweigh the cons and the vendor landscape is rapidly expanding to meet the demand for more training and test data in AI. Increased adoption of simulation techniques will accelerate this trend.

User Advice:

- Identify areas in your organization where data is missing, incomplete or expensive to obtain, thus, currently blocking AI initiatives. In regulated industries, such as pharma or finance, exercise caution and adhere to rules.
- Where personal data is required but data privacy is a requirement, consider synthetic variations of the original data or synthetic replacement of parts of it.
- Begin with the sampling approach and leverage data scientists to ensure statistical validity of the sample and distribution of the synthetic data.

- Mature toward the simulation-driven approach, emphasizing creating agents and processes within a simulation framework to generate permutations of interactions that result in synthetic data.
- Above all, leverage specialist vendors while the technology matures.

Business Impact: Synthetic data promises to accelerate training data development, improve precision, reduce costs and cover more scenarios resulting in more quickly developed and resilient AI solutions. Further, synthetic data can act as a democratizer for smaller players as they try to compete with data-laden tech heavyweights. Privacy restrictions are an additional major driver of this technology with finance and health verticals adopting this approach to "free up" model development efforts. As a result, we see the benefit as "high." Today, we see increased adoption of synthetic data approaches across industries; in particular automotive, robotics, content generation, retail, fraud, finance, defense, and logistics along with early shoots of use in development of synthetic speech and natural language data for NLP applications. Enterprises should expect a rapid growth in the use of these techniques over the next three years.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: AiFi; AI.Reverie; Arcarithm; Bitext; Diveplane; Hazy; Kinetic Vision; Mapillary; Simudyne; TwentyBN

Recommended Reading:

"Cool Vendors in AI Core Technologies"

"Maverick* Research: Use Simulations to Give Machines Imagination"

"Boost Your Training Data for Better Machine Learning"

"Drive Data Scientists' Productivity With Data Preprocessing Techniques"

Blockchain for Data Security

Analysis By: David Mahdi

Definition: Blockchain-enabled data security applications leverage blockchain's decentralization capabilities to offer alternative methods to establish data protection, with minimal reliance on centralized arbiters. Blockchain-enabled data security methods can enhance use cases involving chain of custody ensuring data integrity, as well as encryption, (e.g., offering a decentralized key repository for decentralized PKI).

Position and Adoption Speed Justification: At the core of blockchain is the ability to ensure that participants with no other trust relationship have access to identical ledgers. This property provides

two key data security attributes to the ledger data: integrity and availability. An additional property, confidentiality (i.e., data encryption), is typically done as an additional step to ensure data protection. Data protection methods can be completed on-chain or using integrated off-chain methods, but leverage blockchain technology to ensure all aspects of confidentiality, integrity and availability. However, there are vendors such as ALTR that provide aspects relating to integrity, availability and confidentiality by leveraging blockchain technology.

Overall, leveraging blockchain core decentralization capabilities, combined with complementary data security approaches, offers IT leaders new methods to ensure integrity, availability and, in some cases, transparency.

User Advice: To illustrate a blockchain-based approach to data security, consider ensuring data integrity for a dataset. By storing a representation of the dataset (i.e., a hash) in the blockchain, all nodes will now be aware of the status. Any attempt to change the data will require consensus among the nodes. Therefore, any data logged in the blockchain becomes a part of the immutable decentralized ledger. Common data security approaches that may benefit from a blockchain-based approach, such as PKI, key management and tokenization, can all gain resilience, reliability, transparency and trust due to blockchain's ability to decentralize these functions.

Data security leaders should familiarize themselves with blockchain through early stage research. One such approach is by following publicly known proofs of concept. In doing so, leaders can gain insight into new ideas and approaches that may be relevant. A number of new and well-established vendors are experimenting with data security applications in areas such as:

- Ensuring the integrity of data and/or devices (including things in the IoT)
- Data transparency (e.g., smart contracts or land registries)
- Mitigating trust issues (e.g., distributed/decentralized authority)

Data security leaders should work with developers/architects to establish at least a high-level position on blockchain's relevance and a vision for future adoption. Blockchain-based data security initiatives differ dramatically from legacy business technology and processes. Therefore, data security leaders should take a bimodal approach and experiment with blockchain-based initiatives as Mode 2 projects.

Business Impact: Blockchain has the potential to increase resilience, reliability, transparency and trust in a variety of common data security functions that hinge on centralization, such as PKI, key management and tokenization. Blockchain applied to data security applications offers alternative methods that allow businesses to gain further trust in their data by ensuring integrity and availability. This can be enhanced further by layering in data protection techniques such as data encryption that could be done off-chain.

An example is in securing and sharing public records such as a land registry digital document. The traditional approach is to host the document in a central database maintained by a select number of administrators. This model potentially suffers from weaknesses with resilience and transparency. What is to stop a malicious actor from modifying the land registry? In contrast, if the document or a pointer to the document was stored in a blockchain, then availability, transparency and integrity are

maintained via the distributed cryptographic nature of blockchain. Any change or attempt to change the document is evident and requires consensus among the nodes. Most important, all of these transactions are made public via the nature of blockchain.

This is in direct contrast to traditional approaches that would have the data stored in a central repository that typically doesn't require multiple parties to manipulate the data. As such, Gartner has witnessed increased client interest in leveraging blockchain to establish integrity and overall trust in data.

Finally, due to the absence of meaningful regulation or standards, governance must be exercised to limit risk within organizational tolerance and also must ensure that enterprise risk appetite will allow for experimentation and eventual adoption of the new technology.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: ALTR; Guardtime; IBM; Remme

Recommended Reading:

"Innovation Insight for Blockchain-Enabled Data Security Applications"

"Innovation Insight for Blockchain Security"

"Evaluating the Security Risks to Blockchain Ecosystems"

Privacy

Analysis By: Jie Zhang

Definition: Privacy in China is preserved by a national standard for privacy, a cybersecurity law, and is enforced by other relevant regulations. Personal information for Chinese citizens is defined to include two categories: general and sensitive. The Privacy Standard, the Chinese Cybersecurity Law and the multiple-level protection scheme (MLPS) outlined special data protection practices on both types of personal information. For example, locally storing private data collected in China or data localization is a mandate.

Position and Adoption Speed Justification: The position is adjusted from 2019 as the drivers for hype continue to exist. The rapid adoption of digital business in China (especially mobile payment, large and complex third-party data sharing and processing especially in financial services, online shopping, and news and information content platform) continues to add risks for personal data to be breached or mishandled. The overall trailing privacy practice in society, fraud activities, excessive data collecting and trading, etc., have driven Chinese lawmakers and regulators to establish guardrails for protecting its citizens' privacy. The government effectuated MLPS 2.0, which includes further guidelines on private data protection at the heel of its first Privacy Standard in May

2018 and the first Cybersecurity Law in June 2017 and subsequently drafted a regulation on cross-border data transfers. In early 2019, China also finalized its "Guideline for Internet Personal Information Security Protection" offering additional detailed privacy requirements. These guardrails have a direct impact on how both global and local businesses operate in China. Reactions to Chinese privacy-related topics peaked immediately after the enactment of the law (demonstrated by media and business interest, and Gartner client interactions).

Cases of severe penalties have been continually reported on mishandling or insufficient protection of personal information in 2019. These cases demonstrate the will and wish from the central Chinese government of controlling and regulating personal data protection practices. The pandemic of COVID-19 has also pushed the hacking of personal information to another level. The clarity provided by the Privacy Standard plus MLPS 2.0 continues to provide urgencies on business to pay attention to privacy protection practices. However, it will take time for the overall privacy culture or lack thereof and the associated legal enforcement to mature.

User Advice: Security and risk management leaders should:

- Discover, classify and map data between operations in China and other corporate locations, as it is the necessary first step to prepare for collecting explicit consent and preparing for data localization.
- Incorporate a privacy assessment for the Chinese privacy standard in enterprise information governance by treating it as a parallel, but complementary, effort to General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and other privacy compliance requirements.
- Continuously monitor the development of future guidelines relevant to privacy by working with legal experts that specialize in the Chinese market with strong privacy practices.
- Treat the Chinese Privacy Standard and MLPS 2.0 within the context of the Chinese Cybersecurity Law as privacy requirement is not only an integral part of the law but also guided and enforced by the law in reality.
- Separate data protection and retention for China operations from global information governance as local privacy rules could often be enforced differently from other regions.

Business Impact: Defining and addressing privacy compliance needs support business goals and market access especially for businesses in highly regulated sectors such as financial services or multinational operations expanding in China. Therefore, global business leaders need to rethink their market growth strategy. Additional investment is necessary, or a path of "China for China" strategy is needed as potentially the privacy risks outweigh business benefits; because costs for new IT infrastructure, application architecture, data management and skills will rise. Although the central government and industry-specific agencies continue working on defining details around privacy requirements, compliance risks and potential penalties for violations in China are real and can be significant. For businesses serving the China market, privacy leaders need to consider introducing new roles, new controls and policies to manage Chinese privacy requirements. Near-term privacy management changes from various Chinese authorities (i.e., industry-specific agencies) are also

expected. Therefore, privacy in China has an ongoing impact on monitoring and security audit/assessment as well.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Recommended Reading:

"China's Data Privacy Standard Unfolds Measures for Its Cybersecurity Law"

"Security Assessment Becomes Prerequisite for Transmitting Data Out of China"

"Address Chinese Cybersecurity Law With This Playbook"

"Balancing the Risk of China's Social Credit System for Business Benefits"

At the Peak

Data Breach Response

Analysis By: Nader Henein; Bernard Woo

Definition: Data breach response, augmentation and the associated disclosure are the set of activities required to assess and potentially notify supervisory authorities and — depending on impact — affected individuals when personal data is compromised.

Today, disclosure is mandated by privacy laws such as the European Union's GDPR and exceedingly more U.S. state breach notification laws updated over the course of this past year. Furthermore, these requirements can be found in laws far and wide at regional, federal, state and sectoral levels.

Position and Adoption Speed Justification: The GDPR (Articles 33 and 34) has raised the bar on data breach notification, requiring disclosure to the supervisory authority within 72 hours of becoming aware of a reportable incident. Not only do all 50 states across the U.S. have breach notification laws in place, some, such as New York, have begun amending their laws. Amendments typically both expand the data in scope and requirements surrounding the protection of that data.

The regulatory evolution illustrates the need for organizational commitment and resource allocation. An ongoing process to align the technical and operational elements of incident response with new legal and regulatory requirements. Elevating the capacity to disclose a data breach (to regulators and affected individuals) in a time frame for which many organizations are not prepared today.

User Advice: Security and risk management leaders, including those that oversee privacy programs, must assess their organization's ability to address data breaches in an efficient and timely manner.

Data breach response requires a combination of technical acumen (forensics analysis as to how the breach took place, the number and type of records involved, and appropriate remediation) paired with coordinated organizational processes.

Specifically, those charged with overseeing or managing a data breach response need to assess first and foremost whether an incident, based on the information that has been compromised, has risen to the level of a privacy violation. Details about incidents (not just violations) should be recorded and maintained as some jurisdictions have stringent record keeping requirements.

Personal data breach response should be viewed as a multidisciplinary process that involves:

- Simulated drills to ensure that tasks are well-defined, and responsibilities are clear.
- Coordination and transparency between legal, human resources, security operations, executive management, corporate communications, as well as the organization's privacy team.
- Integration into the larger incident response training, including preparations for new, more stringent breach disclosure and response requirements.

Security and risk management leaders are reminded that as part of a response to a data breach, they should drive reviews into the organization's operations to identify areas that need to be strengthened in order to prevent a reoccurrence.

Business Impact: Data breach response can have a critical impact on the resilience of an organization. Breaches will create significant chaos as key members of the executive team pivot from preexisting priorities to address the reputational, regulatory and likely financial impact of the breach.

With regulations imposing more aggressive fines for data breaches as well as fine reductions when they are handled properly, the financial impact and benefit should not be underestimated. Taking the process one step further, certain draft proposals aim to impose statutory sentences on company directors for egregious or negligent handling of personal data.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BigID; IBM Resilient; OneTrust; RadarFirst; SAI Global

Recommended Reading:

"Market Guide for Digital Forensics and Incident Response Services"

"How to Implement a Computer Security Incident Response Program"

“Toolkit: Security Incident Response Roundtable Scenario for Privacy”

“How to Write a Security Incident Response Procedure Document”

Secure Multiparty Computing

Analysis By: David Mahdi; Bart Willemsen; Brian Lowans

Definition: Secure multiparty computing (SMPC) is a method of distributed computing and cryptography that enables entities (applications, individuals or devices) to work with data while keeping data or encryption keys in a protected state. Specifically, SMPC allows for multiple entities to share insights while working with confidential data.

Position and Adoption Speed Justification: With increasing demands of privacy protection and adequate, contextualized security controls, security and risk management (SRM) leaders struggle to achieve balance between data protection requirements and business objectives. Regulations focused on privacy and data protection further complicate the processing of (personal) data.

Historically, data protection has focused mainly on two states: securing data at rest and in transit. However, with SMPC-based methods and key splitting, it is possible to employ data protection in use. Data protection in use introduces a new paradigm to the arsenal of security methods and enhances traditional security approaches. The application of SMPC extends to combating data residency concerns, for example, balancing a single-point-of-failure risk regarding a cloud service provider’s environment. SMPC can empower cloud key management with the ability to “split” cryptographic keys in a manner such that it ensures protection and privacy in the cloud. Most importantly, it facilitates data sharing for analytics in a protected state, across multiple contributors.

User Advice: SMPC-based solutions offer new methods to ensure scalable, private and secure data processing and sharing. With SMPC just starting to become a reality from a product and solution perspective, a number of new vendors are solving data security and privacy use cases with SMPC-based technology, often in combination with other capabilities. Use cases include:

- Cloud computing (confidentiality with data in a cloud environment)
- Privacy-preserved (personal) data analytics
- Encryption key management
- Cryptographic key protection
- Scalable software-defined hardware security modules (virtual HSMs)
- Secure and private data mining
- IoT security
- Blockchain security
- Analytics of data using proprietary algorithms

Data management strategies that include SMPC-based approaches enable secure and private sharing and analytics of data. For example, an organization that aims to extract value from customer data but has to adhere to strict privacy laws can maintain information value to extract insights while ensuring that the data is kept in an unidentifiable state. SRM leaders should work with developers/ architects to establish a high-level position on its relevance and a vision for the future adoption.

Furthermore, trust in the SMPC algorithm(s) and their respective security posture are crucial to SMPC's effectiveness as a privacy-preserving technology. SRM leaders must continue to gain insight into the technology development to provide trust-invoking transparency.

Business Impact: As organizations face ongoing pressure to ensure that their data is secure and private throughout the data life cycle, SRM leaders will need sustainable, effective and efficient ways to comply and treat risk.

SMPC, while known to academia for a few decades now, is only now starting to become commercially viable.

As volumes of both structured and unstructured data continue to grow, SRM leaders will need scalable, privacy-centric approaches to protect data amid a landscape of maturing data protection regulations. This is particularly important in areas such as cloud, Internet of Things and data mining or monetization.

SMPC can alleviate privacy concerns in the areas of big data analytics, machine learning (ML) and artificial intelligence (AI). SMPC helps SRM and data and analytics leaders to benefit from data insights that are derived from ML and AI while keeping the data secure and private. As ML and AI mature, SMPC will need to account for performance issues with specific algorithms such as recursive algorithms. Overall, SMPC allows for the secure enablement of business, enabling organizations to leverage their data while mitigating security and privacy concerns.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Baffle; CryptoNumerics; Cybernetica; DataFleets; Inpher; Unbound Tech

Recommended Reading:

"The State of Privacy and Personal Data Protection, 2019-2020"

Consent and Preference Management

Analysis By: Andrew Frank

Definition: Consent and preference management platforms consolidate end-user choices regarding how their personal data should be handled. Choices are synchronized across a variety of legacy, active and incoming repositories, both on-premises and in the cloud. The intent is to extend visibility

and control to consumers, allowing them to determine and change at will how much of their data to expose, to whom and for what purpose. This also empowers marketers to respect their choices with a minimum of manual overhead.

Position and Adoption Speed Justification: The EU's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA) and a global wave of privacy legislation initiatives coupled with deprecation of browser-based tracking mechanisms are driving peak demand for consent management solutions. Offerings have evolved rapidly to meet demand but the details of implementation prove challenging for many organizations.

Obstacles include legal frameworks that vary materially by region, compliance requirements that make for challenging customer experience design, and integration challenges that span multiple legacy systems and lack standard metadata definitions and guidelines. Organizations adopting consent and preference management platforms (CPMPs) face the challenge of assembling cross-functional teams consisting of legal, technical, and marketing resources.

CPMP projects are frequently underscoped as vendors overpromise what can be accomplished with out-of-the-box solutions and integrators confront the complexity of managing granular consent options and satisfying rights requests that can affect multiple internal and external datasets. Marketers, meanwhile, seek an elusive balance. Forcing too many privacy choices on consumers can degrade user experience and lead to high opt-out and abandonment rates. Offering too few privacy choices can limit the legal ability to process data to understand customer behavior and offer tailored experiences, or raise compliance questions when data is processed without unambiguous consent. CPMP providers have generally left front-end design solutions to their customers, where applicable skills and experience are in high demand. Lacking such skills, many marketers are tempted by "dark patterns" that attempt to trick or frustrate a user into opting in.

None of these challenges is conducive to a rapid solution. The legislative process is slow and most governments are preoccupied with coronavirus crisis management. Without consistent laws and enforcement, organizations must treat solutions as stop-gap while solution providers and standards bodies struggle to anticipate the details of controversial legislative outcomes. We anticipate a plateau horizon near five years, with an extended journey through the Trough of Disillusionment, as economies rebuild and power struggles among internet giants, privacy advocates, and commercial interests fail to find easy resolutions.

User Advice: Marketing leaders and security and risk management leaders responsible for collecting and using consent should:

- Avoid oversimplifying consent management requirements and assemble sufficient resources from across the organization to document requirements and evaluate solutions.
- Develop a consent matrix that defines types of communications granularly, and port existing customer databases into this new model. Use it to determine whether a packaged CPMP solution is justified by assessing requirements against market options and internal costs.
- Break out consent collection and fulfillment requirements from subject rights request automation and treat them as complementary initiatives.

- Implement a formal review process for consent flow designs and work with designers and customer experience experts to create prototypes and test alternatives.
- Treat consent as a contextual and progressive customer experience. Test and optimize design trade-offs and quantify costs of consent flow options in terms of user abandonment and consent decline rates.
- Shift focus from legal requirements toward user-centric design. Long-term engagement between consumers and brands is only achievable if CPMP aligns with consumer goals and values.

Business Impact: Consumer brands face a growing trust crisis that threatens profitability and depletes brand value. As privacy regulations force brands to obtain advance consent for each instance of personal data processing, the risk of habitual declines threatens to deprive marketers of their ability to offer personalized services and anticipate customer needs based on observed behavior. This further diminishes the value of brands to customers. The commercial impact of privacy regulation hinges on marketers' abilities to craft compliant solutions based on articulating benefits to consumers. CPMPs are thus critical to building a trust-based relationship between consumers and brands that put consumers in control of their personal data. Business benefits include increased brand loyalty, customer satisfaction and retention levels, and competitive differentiation.

Meanwhile, consumer-facing digital platforms such as Google, Facebook, and Amazon are the most visible targets of privacy complaints and have the most at stake as governments contemplate how to reign in their massive personal data collection and processing operations. These providers devote massive resources to honing their consumer consent collection designs and justifications. The outcome of their efforts, along with the success of brands, directly influences whether personalization and ad targeting based on personal data will be concentrated in a digital oligopoly, distributed among brands in competitive markets, or simply disappear.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BigID; Consentua; Crownpeak; LiveRamp; OneTrust; PossibleNOW; Salesforce; SAP; Tealium; TrustArc

Recommended Reading:

"Market Guide for Consent and Preference Management"

"Market Guide for Consent and Preference Management for Marketers"

"Market Guide for Subject Rights Request Automation"

"Survey Analysis: Consent and Preference Management Platform Adoption Remains Low Despite Mounting Privacy Concerns"

“Survey Analysis: European Marketers Favor Short-Term Flexibility in Tech Deployments Over Long-Term Strategy”

“How to Minimize Your Marketing Data Dependence on Amazon, Facebook and Google”

Decentralized Identity

Analysis By: David Mahdi; Michael Kelley

Definition: Decentralized identity services leverage technologies such as blockchain or other decentralized ledger technologies (DLTs) to decentralize an identity system by distributing it across a large number of nodes or participants. Thus, they provide an alternative to siloed legacy IAM architectures by establishing trust in identities and resiliency within the overall system, with little reliance on centralized arbiters or identity stores.

Position and Adoption Speed Justification: Decentralized identity (DID) differs from traditional IAM approaches due to the concept of centralized, versus decentralized, generation and storage of identities. Traditional IAM approaches, storing identity and entitlement data in central authoritative sources can be problematic from the perspectives of liability, security, scalability, reliability and privacy.

A decentralized approach minimizes these problems due to its core architecture being decentralized, distributed and transparent. It has the potential to increase trust, scale and resiliency, possibly with a more equitable and efficient economic model.

Standards are currently emerging, and at a fast rate. However, the market will take time to reach a steady state. However, development and innovation are increasing at a rapid pace, actively supported by financial and government institutions. On the standards front, the WC3 group, along with the decentralized identity foundation, (DIF), have created open standards which DID vendors can use to align their technology and vision with the rest of the market. In addition, the recently launched Trust over IP (ToIP), offers some promise in the area of standardization as well (see “Guidance for Decentralized Identity and Verifiable Claims”).

A growing number of IAM approaches are reflecting blockchain-based enhancements including bring your own identity (BYOI) and decentralized identity. Mid 2019 and early into 2020, saw new entrants into the space such as Mastercard, Microsoft, Ping Identity (acquired ShoCard March 2020) Workday (acquired TrustedKey August 2019). Implementations are still primarily in POC, however, initiatives are gaining traction (such as Verified.Me in Canada).

Decentralized identity now sits at the peak; however, we have extended time to plateau. Practical blockchain-based solutions were overhyped and have made less headway than expected. Furthermore, effective solutions will depend on secure (formerly “privacy-enhanced”) multiparty computing and zero-knowledge proofs, which have longer timescales.

User Advice: IAM leaders should familiarize themselves with decentralized identity through early stage research. In doing so, leaders can gain insight into new ideas and approaches that may be relevant. Ultimately, leaders must base all planning decisions on a clear understanding of the core

differences between decentralized identity and traditional IAM approaches. A number of new and well-established vendors are experimenting with IAM applications in areas such as:

- Identity registration and verification.
- Ensuring integrity of devices (including things in the IoT).
- Enabling identity data sharing while preserving privacy ("consent control").
- Mitigating trust and transparency issues by using the distributed/decentralized model.
- Enhancing the ability to handle identities, attributes and relationships at massive scale.
- Enabling bring your own identity and/or self-sovereign identity. (Self-sovereign identity is another description for decentralized identity, or user managed identity; see "Blockchain: Evolving Decentralized Identity Design.")

IT leaders with an interest in decentralized identity approaches must recognize that leveraging this technology today requires proofs of concept to learn about the technology and, ultimately, the new business models and identity ecosystem that can be realized. Leveraging in market vendors, such as Microsoft, Workday, InfoCert or IBM, is one option to understand the possibilities of decentralized identity applied to their use cases. Customer identity and access management, (CIAM) use cases in particular offer potential for a DID approach.

Business Impact: Ultimately, with decentralized identity, users gain control of their identities and related attributes (i.e., personal information such as address, age and credentials), and service providers will be able to onboard and interact with users with greater speed and confidence. This is in contrast to many online services today, where digital identity and access are siloed, and service providers are forced to horde identity information about users. This has led to data breaches and other security and privacy issues. In the age of GDPR and privacy-conscious consumers, service providers will need to reevaluate their stance on the identity data they store. By leveraging decentralized identity, service providers could liberate themselves from storing sensitive data, instead relying upon assertions generated by identity providers.

Leveraging decentralized identity has the potential to allow service providers to increase security and convenience of access for end users, while reducing exposure to data breaches and potential privacy compliance violations.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: 1Kosmos; Evernym; Hyperledger; IBM; InfoCert; Microsoft; Ping Identity; SecureKey; Sovrin; Trusted Key

Recommended Reading:

"Innovation Insight for Decentralized and Blockchain Identity Services"

“Innovation Insight for Bring Your Own Identity”

“Guidance for Decentralized Identity and Verifiable Claims”

“Top 10 Strategic Technology Trends for 2020: Practical Blockchain”

Digital Ethics

Analysis By: Jim Hare; Frank Buytendijk; Lydia Clougherty Jones

Definition: Digital ethics comprise the systems of values and moral principles for the conduct of electronic interactions among people, organizations and things.

Position and Adoption Speed Justification: Digital ethics remains at the Peak of Inflated Expectations. Digital ethics and privacy remain growing concerns for individuals, organizations and governments. Consumers are increasingly aware that their personal information is valuable, and they’re frustrated by lack of transparency and continuing misuses and breaches. Organizations increasingly recognize the risks involved in securing and managing personal data, and governments are implementing strict legislation in this area.

The coronavirus outbreak has demonstrated the important role of digital ethics in how governments and healthcare organizations are using technology and personal data to address the pandemic. However, no matter how urgent the response to the crisis is, decisions about how technology and data are used could result in more harm than good if those decisions are not grounded in digital ethics. The pandemic has shown that regardless of the hype around digital ethics, many organizations are still not applying them. And, as a result, the innovation hasn’t yet passed the Peak of Inflated Expectations.

Board members and other executives are sharing their concerns about the unintended consequences that the innovative use of technology can have. There is frequent, high-profile press coverage of stories that concern the impact of data and technology on business and society more broadly. More universities across the globe are adding digital ethics courses including the University of Oxford and the University Melbourne that recently launched programs and centers to address ethical, policy and legal challenges posed by new technologies. Government commissions and industry consortiums are actively developing guidelines for ethical use of AI (see “How Forthcoming EU Legal Framework Will Affect Your AI Initiatives”).

User Advice: Business value and digital ethics need not be in conflict. Intention is key. If the only goal is business performance, and ethics is seen only as a way of achieving this goal, this may lead to window dressing. However, if the goal is to be an ethical company, and this leads to better business performance, then this serves all parties, and society more broadly. It will only strengthen the organization, helping you to have an even greater positive influence in the future.

Business and IT leaders responsible for digital transformation in their organizations should:

- Identify specific digital ethics issues, and opportunities to turn awareness into action throughout the various business domains.

- Discuss ethical dilemmas from different points of moral reasoning, such as outcome determinative versus empathy-focused. Ensure that the ethical consequences have been accounted for and that you are comfortable defending the use of that technology, including unintended negative outcomes.
- Elevate the conversation by focusing on digital ethics as a source of business value, rather than simply focusing on compliance and risk. Link digital ethics to concrete business performance metrics.

Business Impact: There are ethical consequences that arise through the use of digital technology in every business domain. Digital ethics should be treated as a tangible business practice discipline rather than an academic discussion. It does not have to be at odds with optimizing business performance. In fact, ethical behavior can have business value in itself.

Areas of business impact include influencing innovation ideas, product development, customer engagement, corporate strategy and go-to-market.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Avanade; Hypergiant; IBM; Microsoft; Salesforce; SAP; SAS

Recommended Reading:

"Data Ethics and COVID-19: Making the Right Decisions for Data Collection, Use and Sharing"

"Digital Ethics: What Every Executive Leader Should Know"

"Digital Ethics by Design: A Framework for Better Digital Business"

"Top 10 Strategic Technology Trends for 2020"

"The CIO's Guide to Digital Ethics: Leading Your Enterprise in a Digital Society"

"Data Ethics Enables Business Value"

"Use Privacy to Build Trust and Personalize Customer Experiences"

File Analysis

Analysis By: Michael Hoeck

Definition: File analysis software analyzes, indexes, searches, tracks and reports on file metadata and file content. FA solutions are offered as both on-premises and SaaS options. FA software reports on detailed metadata and contextual information to enable better information governance, risk management and data management actions against unstructured data.

Position and Adoption Speed Justification: File analysis (FA) solutions assist organizations in managing the ever-expanding repository of unstructured "dark" data. This includes file shares, email databases, content services platforms, content collaboration platforms and cloud-based productivity platforms, such as Microsoft Office 365 and Google G Suite. The primary use cases for FA software for unstructured data environments include:

- Organizational efficiency and cost optimization
- Regulatory compliance
- Risk mitigation
- Text analytics

The desire to mitigate business risks (including security and privacy risks), identify sensitive data, optimize storage cost and implement information governance are key factors driving the adoption of FA software. The hype associated with the growing trend of privacy regulations such as GDPR and CCPA has greatly raised the interest and awareness for FA software. When exposed through the use of FA software, the potential value of contextually rich unstructured data is capturing the interest of data and analytics teams.

User Advice: Organizations should use FA software to better grasp the risk of their unstructured data footprint, including where it resides and who has access to it, and to expose another rich dataset for driving business decisions. Utilize for cleanup of old file shares containing ROT data, which can be defensively disposed of or relocated to optimize data infrastructure. Data visualization maps created by FA software can be presented to better identify the value and risk of the data. This, in turn, can enable IT, line of business (LOB) and compliance organizations to make better-informed decisions regarding classification, data governance, storage management and content migration. For example, apply to regulatory compliance projects, such as CCPA, GDPR or other privacy regulations and readily identify sensitive personal data or key corporate intellectual property data.

Business Impact: FA software reduces business risk and inefficiencies hidden in unstructured data sources often considered "dark" data. They improve management of information governance and operational efficiency practices by:

- Eliminating or quarantining sensitive data
- Identifying access permission issues and protecting intellectual property
- Optimizing storage utilization by finding and eliminating redundant and outdated data
- Feeding data into corporate retention initiatives through the utilization of standard and custom file attributes

FA software also assists in classifying valuable business data so it can be more easily found and leveraged, as well as supporting e-discovery, data migration and analytics.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Active Navigation; Adlib; Condrey; Ground Labs; Index Engines; SailPoint; Stealthbits Technologies; Titus; Varonis; Veritas Technologies

Recommended Reading:

"Market Guide for File Analysis Software"

"Top 5 Emerging Cost Optimization Opportunities for Storage and Data Protection"

"Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy"

Privacy Impact Assessments

Analysis By: Bart Willemsen

Definition: Privacy impact assessments (PIAs) enable organizations to identify and treat privacy risk. Typically conducted before implementing new processing activities and/or major changes, the assessment starts with a quick scan (containing process owner and description, types of data processed for specific purposes, and retention periods per purpose). A full PIA adds envisaged risks to and impacts on data subjects, combined with mitigating measures to ensure a controlled personal data processing environment.

Position and Adoption Speed Justification: Made mandatory through enhanced privacy laws such as the GDPR and the LGPD, PIAs are a recommended best practice for deliberate, secure and purposeful use of personal data. PIAs are slowly transitioning to the mainstream. Often required reactively (for example, as prerequisite to the introduction of new technology), it is best practice to also proactively revisit previous PIAs periodically (at least every year and more frequent with high-risk processing activities). PIAs enable a responsible operation, substantially reducing privacy risk. Additionally, they deliver insight into authorization and access management, purposeful processing, data minimization options, and data life cycle control requirements. With an increasing need for PIAs, there is proportional demand for automation, rather than a manual approach, as they vary in length and complexity. Automated processes and tools — although different in scope and function — are evolving and increasingly available.

Although freemium models have emerged, the administrative burden and (misperceived) operational lack of value has slowed down widespread adoption of structurally implemented PIAs, leaving it only a little post-peak right now.

User Advice: PIAs require the participation of multiple stakeholders, including legal counsel, the privacy officer and the decision-making business (process) owner. Sometimes considered a tedious process, the PIA enables organizations to safeguard individual privacy and in the process avoid reputational damage, and costly, embarrassing or damaging incidents; reduce liability; and enhance informed decision making. It provides insight into the deliberate, purposeful use of personal data and allows organizations to prevent (internal) abuse of such data. Where personal data is used for

purposes that are incompatible with the original processing purpose for which the data was obtained, negative and privacy-invasive effects can be expected.

PIA models and templates, such as those provided by various data protection authorities, continue to vary in scope and granularity. However, automated processes and tools are emerging. Using these tools, organizations create their own internal workflow process to conduct PIAs. Precedent-shaping impactful incidents and (regulatory) rulings will influence adoption of the PIA process internationally, but these take time to have an effect on both market demand and availability.

Recommendations:

- Appoint and mandate business process owners with responsibility over their respective personal data processing activities.
- Require PIAs to be conducted as a mandatory, frequently reiterated activity.
- Include PIAs' results — especially from large projects — in the corporate risk register for monitoring and follow up.
- Demand service providers to conduct DPIAs as part of your ongoing engagement.
- Either provide for a PIA model centrally (e.g., as an internal automated workflow process) or require that it be conducted as a manual exercise, when a less-mature procedure suffices.

Business Impact: Conducting PIAs frequently, such as at the onset of every personal data processing activity implementation and at major changes, or at least annually, maintains control over an organization's personal data management. By implementing the results in the operational environment, organizations may find that they can reduce risk and liability by purging excess data.

The result of a PIA enables regulatory compliance, improves control over personal data throughout the data life cycle, and determines authorization and access management. It collaterally assists in the prevention of (internal) data breaches and personal data misuse or abuse. Importantly, it helps SRM leaders to quantify risk to the individual and timely apply suitable mitigating controls. Conducting PIAs frequently and consistently provides the basis of responsible and transparent personal data management.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: AuraPortal; OneTrust; Privaon; SoftLab; SureCloud; TrustArc

Recommended Reading:

"Privacy as a Partner: Building Citizen Trust in Public-Private Partnerships"

"Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

"Toolkit: Assess Your Personal Data Processing Activities"

Data Classification

Analysis By: Alan Dayley; Bernard Woo; Bart Willemsen

Definition: Data classification is the process of organizing information assets using an agreed-upon categorization, taxonomy or ontology. It enables effective and efficient prioritization for data and analytics governance policies that spans value, security, access, usage, privacy, storage, ethics, quality and retention. Data classification typically results either in the development of a large repository of metadata useful for making further decisions, or applying a "tag" to a data object to facilitate use and governance of data during its life cycle.

Position and Adoption Speed Justification: There are many reasons to classify data, and the decisions about who or what system establishes and enforces classification differ accordingly. Approaches include categorization by data type, owner, regulation or classification by data sensitivity or retention requirements. Data classification momentum continues for digital business transformation, artificial intelligence/machine learning (AI/ML), security concerns and increased regulations and concerns for privacy. Data protection regulations have added needs to classify data around individuals and entities, with privacy-centric classification efforts, and as a foundation for data life cycle management. Datasets residing and migrating across on-premises and multicloud has thrust data classification into the forefront for both organizations and cloud providers.

Data risk and value assessments rely heavily on data classification. For example, security teams use classification technology to assign risk profiles to data. Likewise, the emergent field of infonomics requires classification capabilities to assign value and liability to varying datasets.

Data classification has been around for some time, just not widely adopted. The position in the Hype Cycle reflects a majority of partial or siloed adoption, and still developing capabilities.

User Advice: Data classification attempts can be difficult at best: to identify, tag and store all of an organization's data, without first taking into account the utility, value and risk of that data. To start, organizations should assess information assets for value and risk, for example using infonomics measures. The purpose is to isolate the data that has minimal or no value to the organization, optimize data management costs and address any archival, retirement, destruction, risk and security requirements. Use an ongoing, adaptive and iterative approach instead of one-off or intermittent audits, continued discovery of data assets helps to perpetuate the process and help with cross-organizational engagement. The key is to start somewhere that will have a business impact and build out the data catalog over time.

Data classification must also be an ongoing aspect of changing organizational behavior within the data-driven culture, and be supported by data governance and metadata management. SRM leaders and chief data officers (CDOs) should collaboratively architect and use classification capabilities.

Data classification recommendations include:

- Implement data classification as part of a funded data and analytics governance program.

- Determine organizationwide classification use cases and efforts, and, at a minimum, keep all stakeholders informed.
- Combine privacy regulation adherence efforts with the security classification initiatives overseen by the chief information security officer (CISO). As such, information can be categorized by nature (e.g., what is PII, PHI or PCI), or by type (e.g., contract, health record, invoice). Regardless, records should also be classified by risk categories as to indicate the need for confidentiality, integrity and availability. Finally, records can be indicated to serve specific purposes. Both CIA and purpose classifiers may change during the record life cycle.

Business Impact: Targeted classification, combined with the capabilities of various data management tools, will enable organizations to produce faster, more reliable and efficient data use for discovery, risk reduction, value assessment and analytics. This enables organizations to focus security and analytics efforts primarily on their important datasets. Identity-centric classification efforts can assist when managing concerns for the European General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other privacy regulations.

Classification enables CDOs to drive information asset management as a value-adding opportunity to support better business outcomes, rather than being an approach driven by compliance and records-keeping requirements. In addition, CDOs, CISOs, compliance and other involved functions should work with each other and other pertinent functions to ensure mutual awareness of classification activities.

Data classification can be used to support a wide range of use cases:

- Privacy compliance
- Risk mitigation
- Master data and application data management
- Data stewardship
- Content and records management
- Data catalogs for operations and analytics
- Data discovery for analytics and application integration
- Efficiency and optimization of systems, including tools for individual DataOps

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Boldon James; Collibra; Dathena; IBM; Informatica; Microsoft; Netwrix; OpenText; Titus; Varonis

Recommended Reading:

“How to Overcome Pitfalls in Data Classification Initiatives”

“Ignition Guide to Data Classification”

“Building Effective Control Documents for Sensitive Data Classification and Handling”

“Market Guide for Enterprise Data Loss Prevention”

“How to Successfully Design and Implement a Data-Centric Security Architecture”

Sliding Into the Trough

Format-Preserving Encryption

Analysis By: Brian Lowans; Joerg Fritsch

Definition: Format-preserving encryption (FPE) is used to protect data at rest and in use, as well as when it’s accessed through applications, while maintaining the original data length and structure. It’s used to protect fields in an increasing number of relational database management systems (RDBMSs), data warehouses and NoSQL databases. FPE is an important anonymization technique for data protection and privacy, minimizing the risks of hacking or insider threats, and compliance requirements to control access by administrators and users.

Position and Adoption Speed Justification: Adoption is increasing, due to the fast-growing need to provide data protection and privacy, in compliance with legislation such as the General Data Protection Regulation (GDPR). Organizations increasingly need to analyze data, while keeping it anonymized. The ability to mix the implementation of FPE with data masking is also increasing its dynamic adoption for different use cases.

User Advice: FPE is typically used across a variety of RDBMSs, data warehouses and NoSQL platforms, such as Hadoop, Cassandra and MongoDB. It can be used to protect data at the point of ingestion, storage in a database or access through applications. It is increasingly being deployed to protect data being stored or processed in cloud-based data warehouses and databases. However, it is still a blunt-force access control, and, when applied, it will protect data wherever it resides or accessed. Authorized users with application or database access privileges will have access to the data in clear text.

Hence, when implementing FPE, organizations should also consider tools to monitor and audit all user and administrator access to sensitive data, with database audit and protection tools (DAP). They should also use data loss prevention (DLP) to monitor data movement across endpoints. Any clear-text access to sensitive data may result in that data being stored in other data stores; hence, security policies must be coordinated across all data silos. A good security best practice is the segregation of duties (SOD) of database administrators (DBA) from security controls. DBAs should not be responsible for FPE, and should be managed as part of an enterprise key management (EKM) solution. The National Institute of Standards and Technology (NIST) published standard for FPE describes several algorithm modes in Special Publication 800-38G; however, only the FF1

mode has been approved. Some implementations of FF3 mode may still be accepted. When considering FPE, identify the following:

- What data fields need to be protected in accordance with perceived risks, threats and compliance requirements?
- Do the field lengths need to be maintained or protection only applied to part of a field?
- Should FPE be combined with DAP?
- What will be the adversarial impact of encryption on application functionality?
- Are transparent data encryption (TDE), tokenization or dynamic data masking (DDM) appropriate alternatives to FPE?
- How will FPE fit into an EKM approach?

The most common deployments focus on specific types of regulated data. FPE can replace the whole string within a field, or just a part of the field, to maximize functionality of applications, while maintaining anonymity and without requiring schema changes to databases. Some vendors offer FPE with added features of DDM, where the whole field can be decrypted on-the-fly and then part of a field can be masked on presentation to the application user to offer more flexible access policies.

Review how FPE interfaces with applications, and establish whether user identities can be employed to approve if fields are decrypted. Evaluate any impact on performance and functionality of applications accessing the database. Be aware that other security and database functionality, such as data discovery, can be affected.

Business Impact: The NIST standard for FPE has enabled its acceptance by organizations to address evolving compliance and threat landscapes, without having to extensively modify databases or applications. It provides a strong and agile method to prevent unauthorized user access to data on-premises and, increasingly, in public cloud service platforms. This will help meet data protection and privacy regulations and data residency requirements to protect personal, health, credit card and financial data, as well as data breach disclosure regulations. FPE should be deployed to implement policy rules for user access in coordination with other security controls, according to Gartner's data security governance (DSG) framework.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Comforte; Dataguise; IBM; Informatica; Micro Focus; Oracle; PKWARE; Protegrity; SecuPi; Thales eSecurity

Recommended Reading:

“Use the Data Security Governance Framework to Balance Business Needs and Risks”

“Develop an Enterprisewide Encryption Key Management Strategy or Lose the Data”

“Market Guide for Data-Centric Audit and Protection”

“Prioritize Enterprisewide Encryption for Critical Datasets”

“Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization”

Personification

Analysis By: Andrew Frank

Definition: Personification allows marketers to deliver targeted digital experiences to individuals based on their inferred membership in a characteristic customer segment rather than based on knowledge of their personal identity.

Position and Adoption Speed Justification: We estimated Personification to hit the Peak of Inflated Expectations in August 2019 when Google announced an initiative called Privacy Sandbox. Based on years of Google research, Privacy Sandbox proposed “a new way that browsers could enable interest-based advertising on the web, in which the companies who today observe the browsing behavior of individuals instead observe the behavior of a cohort (or ‘flock’) of similar people.” Five months later, Google raised the profile of Privacy Sandbox by announcing it would abandon third-party cookies in its Chrome browser within two years, dealing a critical blow to marketers’ ability to track users across the web. Google’s proposal describes numerous concepts, such as differential privacy and federated learning in the browser, to infer people’s membership in interest groups, while only exposing cohorts to marketers in blocks of thousands of otherwise anonymous users. This has led to a broad and animated public discussion of technical and conceptual details associated with privacy-preserving targeting.

Although Privacy Sandbox is mostly aimed at targeted advertising, its applications extend to any web-based instance of personification. The privacy issues it seeks to resolve are so charged that, despite a wave of enthusiasm over its visionary scope, the proposal was condemned almost immediately by the Electronic Frontier Foundation as bad for privacy.

Google is far from the only player promoting anonymous data solutions based on aggregate profiles to marketers. Independent data brokers and ad tech companies are quick to point out that Google is not a disinterested party in the development of new web standards and that persona-based targeting doesn’t necessarily require new technology. Marketers today are pursuing alternatives to personal targeting based on collective behavioral insights from advanced analytics and machine learning. They’re also relying on more generic anonymous data, such as regional location, type and state of device being used, session-based behavior signals, and contextual factors like time-of-day and local weather. However, achieving and measuring success with these tactics can be difficult, leading many marketers to focus instead on consensual tracking, however limited. Others retreat to marketing approaches that focus on basic keyword-style contextual targeting, prominent sales incentives and generic creative appeal.

Personification strategy becomes even more challenging under pandemic conditions that lack precedents for predicting behavior and drive marketers to cut costs and focus on tone and utility messaging above all. These factors lead to a picture of personification descending rapidly into the Trough of Disillusionment.

User Advice: Marketers must:

- Study or appoint someone to study, report on and possibly engage with the Privacy Sandbox and similar privacy-preserving targeting standards initiatives.
- Reevaluate personalization strategies to focus on content designed to help anonymous consumers in ways that encourage engagement and require less data to provide relevance.
- Make a clear-eyed assessment of the degree and circumstances under which customers and prospects are likely to grant broad consent to tracking and profiling. Assure that customers who decline consent still receive valuable experiences. Beware of tactics that attempt to gain consent with financial incentives or subversive design patterns.
- Use segment discovery analytics and machine learning techniques to maximize the value of contextual data.
- Make sure that personified segments are free of personal data and can't be combined with other data to identify (or reidentify) an individual.

Business Impact: Personification impacts three areas of marketing:

- Targeted advertising is strongly impacted by new restrictions on the flow of personal data. By shifting reliance to nonpersonal data, personification has the potential to restore value lost to the digital advertising supply chain. This shift in reliance could also prevent further consolidation of market power among platforms most likely to gain large-scale consent to ad targeting based on massive audience engagement (e.g., Google, Facebook and Amazon). However it could also convey new power to browser and app platform providers (Google and Apple) that require new forms of oversight.
- Direct marketing (such as email and mobile messaging) is increasingly subject to legal consent restrictions. Personification can reduce the extent of personal data required for profiling, reducing resistance to consent, while continuing to optimize relevance and engagement.
- Many personalization solutions assume both presence and consent to use visitor data for personalization. Personification can be applied in a broader range of situations and content strategies with less risk.

Personification is an attractive area of research for machine learning because its goal is to make strong inferences from data that is harder to interpret than traditional demographic and behavioral datasets. Its utilization of publicly available data, including public posts and profiles on Twitter, LinkedIn, Instagram, etc., may expose new regional and generational disparities in privacy norms.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Adobe; Adworthy; Amobee; Analytic Partners; BloomReach; Google; Merkle; Oracle; Salesforce; Segment

Recommended Reading:

"Use Personification to Balance Personalized Marketing With Privacy and GDPR"

Privacy by Design

Analysis By: Bart Willemsen; Nader Henein

Definition: Privacy by Design (PbD) is a set of privacy principles that are mandatory in certain jurisdictions, including Europe and Canada. PbD is about protecting privacy proactively by embedding it often and early in technology (e.g., application or customer interaction design), as well as into procedures and processes (through, for example, privacy impact assessments). There is no commonly agreed-upon definition of PbD, though one of the more widely used definitions is that from the Information and Privacy Commissioner (IPC) of Ontario, Canada.

Position and Adoption Speed Justification: Privacy by Design is not a new concept. The term was introduced in the 1990s, but widespread recognition beyond privacy professionals only came when the IPC of Ontario described seven key elements: proactivity, privacy by default, privacy embedded into design, full functionality, end-to-end security, visibility and transparency, and user centricity (see Privacy by Design).

In the U.S., a report by the Federal Trade Commission (FTC) from 2012 is the most visible initial support for the PbD principle. Regulatory guidance is expected to be published from time to time.

The EU's General Data Protection Regulation (GDPR) of 2018 requires "data protection by design and by default," implying a PbD approach to all processing of personal data. Privacy professionals and product vendors have since intensified the debate as to how PbD is best implemented, justifying a position postpeak. With time it is expected that precedent shaping rulings will bring further insight. Meanwhile, vendors have added statements in their go-to-market approach like "the products are designed with PbD in mind," although sometimes with little reference material to support the claim. Ultimately, as privacy preserving capabilities become a more organic part of the development and architecture process, the need for PbD increases as does the benefit rating.

User Advice: Tackle Privacy by Design in manageable steps, a wholesale shift will be too much to handle. Privacy by Design is a cultural change about the processing of personal data. This pertains both to existing operations and to innovations. Through business process reengineering, existing operations may be adjusted. Especially in innovative developments and new processes, the change begins by asking questions, such as:

- Can we achieve the purpose set out by using less personal data?

- Can we end the personal data life cycle earlier?
- Can we provide the same functionality or customer experience without using the identifiable data?
- Does the customer understand what we are processing about them and why?
- Can we adequately protect what we process?

Apply PbD principles first when developing information architecture for personal data from the ground up, but also when evolving and maintaining an existing processing activity (ultimately applying PbD at the company level). Gartner provides a primer, in addition to the seven foundational principles (see “Build for Privacy”).

Systems should be designed so that the collection of potentially privacy-sensitive data is transparent to the data subject. Some technology-focused ideas for implementing PbD are reduction in amounts of personal data and retention (data minimization); working on the original data (rather than copies); and applying pseudonymization where possible, alongside adequate authorization and access controls. Evaluate the risks of reidentification and traceability, and include data location in your considerations. Moreover, implementing PbD can result in organizational and procedural changes such as designating a privacy officer with reach, procurement activities for new IT services or frequently conducting privacy impact assessments.

Expect consumers, employees and citizens, as well as new privacy laws, to pick up the idea of PbD, and assess the necessity of applicability to your organization. Change your development and maintenance processes to include reviews of the privacy design.

Business Impact: Today, privacy is where security was a decade ago: bolted on, rather than built in from the beginning. Experience from security professionals tells us that fixing issues after the development of a product is many times more expensive than getting it right from the start. The same applies to privacy controls. When such controls are built in from the very beginning, they can assist and enable consumer trust, help to prevent violations of privacy rights (such as costly data breaches) before they occur, and reduce their damage if they do (such as fines or brand damage). This is particularly relevant in the context of the Internet of Things. As so many new things are designed, now is the right time to design them from the ground up with privacy and the protection of any personal data in mind.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Recommended Reading:

“Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria”

"Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus (COVID-19) Outbreak by Focusing on These 7 Areas"

"Preserve Privacy When Initiating Your IoT Strategy"

Privacy in Asia/Pacific

Analysis By: Bernard Woo

Definition: Privacy regulatory development in the Asia/Pacific region is gathering momentum. Individual privacy rights are progressively being recognized through new legislation, reform of current laws, and/or increased enforcement activities. The Asia/Pacific Economic Cooperation Cross-Border Privacy Rules (CBPR) added another member country as it seeks to be adopted as the default framework for transborder data flows in region. Several countries in region are leading the adoption of 5G technology, which will greatly increase the amount of personal data processed.

Position and Adoption Speed Justification: The privacy regulatory landscape in region is uneven, though evolving. Jurisdictions with privacy laws include Australia, Hong Kong, Malaysia, New Zealand, Philippines, Singapore and Taiwan. Australia is introducing additional rights for individuals via the Consumer Data Right. Several others, such as Hong Kong, New Zealand and Taiwan (which has delayed enforcement) have signaled intent to reform legislation within the next three years, with requirements expected to become more stringent (for example, mandatory breach reporting). Malaysia issued a public consultation in early 2020 to review its law; one highlighted topic was transborder flow of personal data. Thailand is expected to begin enforcing its Personal Data Protection Act mid-2021. Vietnam began enforcing its Cybersecurity Law, which includes data localization requirements around personal data processing.

The Philippines, with a mature legislation in place since 2012 though enforcement activities have been minimal, became the ninth country to join the CBPR, a framework that supports transborder flow of personal data.

User Advice:

- Security and risk management (SRM) leaders should monitor regulatory activities and developments closely over the next three years to respond in the most effective and expedient fashion. Note that such activities may involve adjacent laws like those regulating cybersecurity activities as well as include data localization requirements.
- Efforts around new laws or legislative reform show a preference toward the model provided by European Union (EU)'s General Data Protection Regulation (GDPR). SRM leaders should therefore lead their organizations in developing a privacy program using GDPR requirements as guidance.
- One key element of such a program is the conducting of risk assessments. SRM leaders must lead their organization to adopt the completion of privacy impact assessments (PIAs) of personal data processing activities. These must especially be done when there are changes in such activities. Completed PIAs should then be revisited on a regular basis to determine whether new risks have arisen.

- Since not all countries in the region have data protection laws in place, SRM leaders should extend beyond privacy considerations and drive implementation of security investments to ensure adequate protection of personal data.
- In the same vein, SRM leaders should ensure there is an incident management program in place to detect, manage and report on potential breaches at the earliest opportunity.

SRM leaders cannot just focus on internal operations, they need to drive focus on active, day-to-day management of third-party risks where service providers are used to process personal data; do not rely on contractual terms alone.

Business Impact: Given the complexity in the regulatory landscape, organizations operating in Asia/Pacific should have a dedicated, senior role in region (for example, regional privacy officer) to lead the development of a privacy program focused on the unique regional requirements.

This is particularly important since several countries in region (Australia, China, Japan, Singapore, South Korea) are expected to be leaders in adopting 5G, the next generation wireless technology. 5G promises to significantly increase the amount of personal data processed and potential attack surface.

Privacy programs therefore can no longer be focused on "the minimum needed for compliance." Organizations should build privacy programs around the purposeful processing of data, using only the minimum of data needed for identified purpose(s), and implementing controls over the entire data life cycle to both secure data as well as protect individual privacy. This will position organizations to meet the expectations in law and earn the trust of customers.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Recommended Reading:

"Build for Privacy"

"Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

"Use These Frequently Asked Questions When Starting a Privacy Program" 9

"Privacy as a Partner: Privacy as a Partner: Building Citizen Trust in Public-Private Partnerships"

"Reduce Privacy Risks When Using 5G Products and Services"

PHI Consent Management

Analysis By: Mike Jones

Definition: Protected health information (PHI) consent management is a system, process and set of policies for consumers to determine what health information they permit their care providers to access or exchange. It enables individuals to affirm participation in patient portals and health information exchanges (HIEs), and to establish and dynamically update granular PHI privacy, access and usage preferences.

Position and Adoption Speed Justification: Gartner predict that by 2022, half of the planet's population will have its personal information, which incorporates PHI, covered under local privacy regulations in line with the General Data Protection Regulation (GDPR), an increase from 10% today.

With the move to a more collaborative and citizen-centric care environment, it is more essential than ever to balance legitimate privacy concerns with the benefits of sharing PHI. The final ONC rule or 21st Century Cures Act supports patients' access to their EHI in a form that is convenient for patients. This means making it accessible through the adoption of standards and certification criteria and the implementation of information-blocking policies that support patient electronic access to their health information at no cost. The intention is that consumers have full transparency on how their electronic health information is being accessed, shared and used at all times and that EHR and other system vendors do not block access

Today, most consent management in healthcare is still done on paper, or in disparate systems of record such as the EHR or CRM. Consent management projects will be driven by a strong collaboration between those concerned with policy and those concerned with the technological implications. The privacy needs of HIEs, accountable care, and patient-centered healthcare movements will continue to drive industry interest in consent management going forward.

PHI consent management is now a key architectural building block for many HIE initiatives, and adoption will continue to increase in relevance.

In the U.S., PHI is a construct that is part of the HIPAA law. In other regions, PHI may be referred to as personal information or identifiable information as part of regional data protection legislation. We have seen this universal capability for consumer-directed consent of health data across the health and care ecosystem appear in many regional digital care strategies and target architectures in recent years..

User Advice: CIOs, CMIOs and CNIOs and those involved in privacy, security and compliance within HDOs and HIEs should promote policies to manage consent and limit the disclosure of PHI.

In the EU for example, the GDPR will effectively mandate this requirement for member states and their health organizations. They need to be asking what kind of consent management systems will be needed, and capture and enforce the dynamic preferences of their consumers and patients. HDO CIOs will also need to make their legacy systems more privacy-aware. Any participation in an HIE should be based on a clear understanding of the policies for consent management, including whether those policies will be enforced centrally by the HIE, or the enforcement is a requirement of the end subscriber.

Business Impact: Open and transparent exchange should enable the permitted use policies to be retained as PHI moves among healthcare entities. This means that the intended use policies, for

which the disclosing HDO remains accountable, should not be overridden by downstream, less restrictive, permitted use policies in other entities. This will require HDOs to ensure that the "purpose of use" is built into their interoperability capabilities and that all business agreements between entities are compliant with varying patient preferences.

Most HIEs have implemented general opt-in or opt-out models — without these highly granular controls — based on federal and state level legislation. The benefit rating reflects the fact that, without effective PHI consent management, it will be difficult to scale the secondary use of health data for key high-value and transformational initiatives. These might include precision medicine, genomics medicine and the use of consumer/citizen-generated data, alongside clinical datasets for advanced analytical endeavors such as machine learning.

We predict that by 2025, 25% of U.S. HDOs will have implemented granular patient consent, but meaningful enforcement will remain a challenge.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Deloitte; Global Public Inclusive Infrastructure (GPII); InterSystems; IQVIA; Jericho Systems; OneTrust; Optum; ZeOmega (HealthUnity)

Recommended Reading:

"Healthcare Provider CIOs: Get Control of Patient Data Across All Partners"

"Healthcare CIOs: Prepare for Granular Patient Consent"

"Business Drivers of Technology Decisions for Healthcare Providers, 2020"

"Market Guide for Health Information Exchange Platforms"

"Cool Vendors in Privacy 2020"

"Healthcare Industry Hot Topic: Debating the U.S. ONC Interoperability and Information-Blocking Rule"

Mobile Threat Defense

Analysis By: Dionisio Zumerle

Definition: Mobile threat defense (MTD) solutions protect organizations from threats on iOS and Android mobile devices. MTD solutions provide prevention, detection and remediation at the device, network and application levels.

Position and Adoption Speed Justification: Enterprises adopt MTD solutions to counter mobile threats. Most often they integrate MTD with their UEM, to increase their security capabilities. However, organizations increasingly use MTD on unmanaged devices, such as in BYOD scenarios. The main use cases that drive adoption are mobile phishing, mobile endpoint detection and response (EDR), app vetting and device vulnerability management.

MTD solutions have reached a level of maturity that makes them suitable for wide enterprise adoption. After a period of intense innovation, MTD innovation has slowed down. In addition to innovation to counter the evolving mobile malware, innovation also focuses on improving the MTD user experience on the device, for example, when providing phishing protection.

MTD adoption has been slower than what the mobile security hype purported, as the industry awaited highly visible or publicized mobile breaches that did not occur. Still, regulated industries and enterprises with high-security requirements have adopted MTD solutions. In their attempt to build a unified endpoint security (UES) offering, endpoint protection platform (EPP) vendors have acquired smaller MTD vendors, others partner with stand-alone MTD vendors, while recently some EPP vendors have been introducing their own MTD homegrown solutions. The availability of MTD through EPP vendors has made adoption easier for enterprises.

User Advice: In addition to a basic security baseline that the average UEM can provide, organizations should perform application vetting and device vulnerability management. Where the current tools do not suffice to do so, enterprises should adopt MTD solutions to improve endpoint security hygiene. Device vulnerability management complexity is particularly accentuated where enterprises operate large fleets of Android devices and these organizations should prioritize the adoption of MTD.

Enterprises that have chosen an unmanaged approach should look into MTD to protect their infrastructure from threats from unmanaged mobile devices. For example, certain MTD tools integrate with Microsoft Outlook, Microsoft Office 365 suite, as well as other popular enterprise suites and managed enterprise apps to provide ZTNA functionality on unmanaged devices.

Increasingly mobile devices are involved in advanced attacks, sometimes as part of a broader attack. For example, mobile phishing attacks can obtain account credentials that an attacker can reuse against an enterprise API, or on a corporate laptop. Because of the current lack of visibility on mobile devices, most organizations never identify these portions of the attack. MTD solutions, stand-alone or as part of a broader EDR or UES deployment, can improve detection of attacks against enterprises.

Business Impact: Because mobile security issues have rarely led to spectacular breaches, enterprises adopting MTD sometimes have difficulty in identifying positive impact. Enterprises have two areas where MTD tools can immediately demonstrate value. The first is device vulnerability assessment where MTD solutions can be used to identify unpatched and vulnerable devices and rank them in terms of severity. The second area has to do with reducing app risk: MTD solutions can identify apps that conflict with an enterprise's security and privacy policies, even when these applications are not malicious. Enterprises in regulated industries such as financial services, insurance, healthcare, government and energy, as well as enterprises with high-security requirements, such as defense contractors and consulting firms are typical adopters of MTD.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BETTER Mobile Security; Check Point Software Technologies; Lookout; Microsoft; Pradeo; Sophos; Symantec; Wandera; Zimperium

Recommended Reading:

"Market Guide for Mobile Threat Defense"

"When Android Is Secure Enough for the Enterprise"

"iPhone and iPad Security FAQs"

"Advance and Improve Your Mobile Security Strategy"

Cloud Data Protection Gateways

Analysis By: Brian Lowans

Definition: Cloud data protection gateways (CDPGs) may deploy a combination of forward or reverse proxy and API adapters to public cloud software as a service (SaaS) providers. They apply encryption or tokenization to structured or unstructured data as it flows through the gateway to the SaaS provider. CDPG protection is also provided by some cloud access security broker (CASB) products. CDPG mitigates inappropriate access to data that could lead to a breach and helps meet data residency requirements for data protection and privacy.

Position and Adoption Speed Justification: CDPG continues to evolve, and to restrict access by application users to data to address data residency and privacy regulations. Vendor products are continuing to evolve separately from CASB by focusing on preventing access by the SaaS providers. They offer specific adapters to SaaS that include Salesforce, ServiceNow, Box, Dropbox, G Suite, Office 365 and Workday.

User Advice: CDPG can provide encryption or tokenization of structured and unstructured data and integrate with enterprise key management (EKM) or bring your own key (BYOK). Review broader organizational needs for data protection and privacy by reviewing any CDPG implementation as part of a data security governance (DSG) assessment. A few of the CDPG vendors also offer additional security capabilities or integrations as a CASB or integration with EKM. However, security leaders must be aware that:

- Tokenization and encryption require a backup key management product to avoid digitally shredding the data in the event of a software or hardware failure, or loss of encryption keys or the tokenization dictionary.

- CDPG products, which offer field or object-level protection of SaaS applications, apply specific adapters or APIs for each SaaS application. Plan for ongoing support of the connector. As cloud providers update their applications, updates to the proxy data protection mappings are likely to be required. However, there may be delays for software updates that, in some cases, could be less efficient for on-premises appliances.
- Some custom-made CDPG encryption algorithms can preserve search and sort functionality; however, they may not meet security standards. Strong data protection techniques will not preserve alphabetical sorting. For example, when protecting customers' names in large lists in Salesforce, it may be desirable to preserve alphabetical sorting.

Security leaders should evaluate trade-offs between security risk and business functionality:

- Minimize the use of tokenization or encryption of fields and files, where possible, to avoid loss of analytics and search and sort functionality. These will also break any SaaS-based calculations performed on numeric fields (and break the application entirely if field mappings are misaligned). Thus, although protection of a credit card number, U.S. Social Security number and other government identifiers may make sense, protection of other numeric fields, such as sales figures, will interfere with SaaS-based calculations (such as roll-ups of sales projections).
- Expand the evaluation beyond encryption services to additional services — such as data loss prevention (DLP) and data centric audit and protection (DCAP) — for user activity monitoring, auditing and logging.
- Evaluate alternatives — for example, the use of endpoint or cloud file-sharing encryption products. Consider that many SaaS providers are adding native encryption capabilities that may be enough. The pros and cons to each approach will depend on the ability to prevent access by the SaaS provider or even the security vendor.

Some CDPG products integrate with native SaaS encryption products using BYOK. However, BYOK is managed separately in terms of key management and policy rules, compared with the proxy or API application of encryption. Whenever possible, look for integrations of EKM as part of an enterprisewide strategy.

Business Impact: Enter into short-term contracts, because CDPG is likely to continue its evolution to integrate more tightly with platforms such as O365, and others becoming integrated with on-premises proxies and data security products. CDPG should be implemented as part of a broader set of security controls via the DSG framework, to assess the trade-offs in deploying CDPG against a CASB, and against native SaaS encryption. The deployment of reverse proxy products can result in some application incompatibilities, as well as impacts on performance and latency.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Bitglass; Broadcom; CipherCloud; eperi; Ionic Security; McAfee; Micro Focus; Netskope; Protegrity; Rohde & Schwarz

Recommended Reading:

"Magic Quadrant for Cloud Access Security Brokers"

"Use the Data Security Governance Framework to Balance Business Needs and Risks"

"Key Management as a Service Exposes Different Risks to Data in Public Clouds"

Privacy Management Tools

Analysis By: Bart Willemsen

Definition: Privacy management tools help organizations conduct privacy impact assessments; facilitate compliance documentation, like records of processing activities (ROPAs); guide consent, preference and privacy rights management; and check processing activities against requirements of privacy regulations. These tools may analyze and document personal data flows (for example, the nature of the data, purpose of processing and the data controller), support authoring and distribution of privacy policies, and track user awareness and third-party risks.

Position and Adoption Speed Justification: Privacy management tools are increasing in both number and distinctive variety. Vendors offer either a compliance-driven solution, a data-focused solution or a combination of both. Maturing privacy requirements globally have driven organizations to identify specific privacy requirements and compliance needs, creating substantial demand. This has driven rapid development in the emerging vendor space. The solutions offered vary in the combinations of functions and features, and therefore serve increasingly different organizations' risk treatment programs. Tools in related areas (for example, security breach notification tools) will, in part, be replaced by more holistic solutions that encapsulate similar features.

Comprehensive (privacy and risk) management tools and consulting services are priced prohibitively for many privacy officers, who usually have only a limited budget, which drives an increased interest in specialized (and less expensive) privacy management solutions. Hence, purpose-built (modular) privacy management tools have emerged that focus on fast deployment and usability. As the market is mostly dominated by relatively young vendors, the offerings are constantly evolving and focus on client requirements, such as universal consent management or data mapping.

User Advice: As organizations process more personal information per capita while facing an increasingly complex set of privacy regulations, security and risk management (SRM) leaders should prioritize dedicated tool support. Ideally, tooling supports compliance with both oversight, documentation and transparency, and offers integration with associated platforms such as data-centric audit and protection (DCAP) or mobile device management, where control over personal data throughout its life cycle is in scope. Wherever possible, SRM leaders should participate in related security, risk and compliance initiatives to achieve efficient spending across these disciplines, and ensure that deployed tools sufficiently cover privacy demands. After all, various stakeholders require information dashboards with differently presented information, essentially derived from the same subsystems. If this is not possible (for example, because requirements are too different, or license costs are too high), then SRM leaders should evaluate dedicated privacy management tools.

Privacy management tools must not be confused with security tools. The protection of personal data by application of security technology is only one aspect of a privacy management program. However, privacy management capabilities (such as data mapping, impact and compliance assessments, personal data lineage and life cycle visualization capabilities, and consent and preference management) may become collateral in reports and dashboards of security-focused products, such as in DCAP. Moreover, there is an ongoing overlap and combination of management and control capabilities found in currently available privacy solutions. Overall, privacy management tools facilitate compliance reporting via dashboarding and documentation. The SRM leader's business case for deployment of security controls and mitigating measures such as cloud access security broker (CASB), enterprise mobility management (EMM) and data loss prevention (DLP) is strong. It will be even stronger if they can demonstrate how those reduce privacy risks. Look for privacy management vendors that integrate with various vertically connected solutions.

Business Impact: Privacy management tools improve information governance in areas where personal information is processed (for example, in HR management, CRM and marketing). The available capabilities enable business management to take accountability for choices made in data processing activities, help architect the data life cycle, and help demonstrate compliance. SRM leaders in organizations that operate in multiple jurisdictions especially benefit from these capabilities when facing different requirements. The same benefit exists when operating in regulated industries, such as healthcare and financial services, and in regulated jurisdictions like the EU, or when facing U.S. state privacy requirements like the California Consumer Privacy Act. Two points of concern are awareness of persistent (personal) data existing in a near-borderless digital ecosystem; and international transfers of personal data, as in XaaS and cloud computing scenarios. Both bring the need to document data flows and manage contractual privacy agreements. Finally, there are early indications that multiple privacy tools, developed for very specific use cases, are starting to converge toward more comprehensive privacy management platforms that can replace fragmented current solutions.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Beyano (DPOrganizer); DataGrail; OneTrust; OpenText; SECURITI.ai; TrustArc; WireWheel

Recommended Reading:

"The Impact of Privacy on Procurement and Vendor Selection and Control"

"Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy"

"Predicts 2020: Embrace Privacy and Overcome Ambiguity to Drive Digital Transformation"

Climbing the Slope

Data Sanitization

Analysis By: Rob Schafer; Christopher Dixon

Definition: Data sanitization is the disciplined process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered (see International Data Sanitization Consortium).

Position and Adoption Speed Justification: Growing concerns about data privacy and security, leakage, regulatory compliance, and the ever-expanding capacity of storage media and volume of edge computing and IoT devices make robust data sanitization a core C-level requirement for all IT organizations.

This requirement for comprehensive data sanitization should be applied to all devices with storage components (e.g., enterprise storage and servers, PCs, mobile devices, and increasingly, edge computing and some IoT devices). Where organizations lack this robust data sanitization competency, it is often due to handling the asset life cycle stages as isolated events, with little coordination between business boundaries (such as finance, security, procurement and IT).

For mobile devices, a remote data-wiping capability is commonly implemented via a mobile device manager (MDM). Although such a remote capability should not be considered a fail-safe mechanism, reliability should be adequate for a significant majority of lost or stolen mobile devices.

User Advice: Follow a life cycle process approach to IT risk management that includes making an explicit decision about data archiving and sanitization, and device reuse and retirement.

Implement policies that assign explicit responsibility for all sensitive or regulated data-bearing devices to ensure that they are properly wiped or destroyed at the end of their productive use.

Collaborate with data sanitization stakeholders (e.g., security, privacy, compliance, legal, IT) to create appropriate data sanitization standards that provide specific guidance on the end-to-end destruction process, based on data sensitivity.

As different media (such as magnetic HDD storage vs. semiconductor-based NAND flash memory) require different sanitization methods, ensure your IT asset disposition (ITAD) vendor provides a certificate of data destruction with a serialized inventory of the data-bearing assets sanitized. Include a clause within your ITAD contract giving you the right to audit the ITAD vendor's data sanitization processes/standards to ensure its compliance with your security and industry standards (e.g., NIST 800-88).

Regularly (e.g., annually) verify that your ITAD vendor consistently meets your data sanitization security specifications and standards.

Understand the security implications of personal devices and plug-and-play storage. Organizations that have yet to address portable data-bearing devices (e.g., USB drives, IoT devices) are even less prepared to deal with these implications.

Consider using whole-volume encryption for portable devices and laptops and self-encrypting devices in the data center.

Consider destroying storage devices, versus reusing them, if they contain highly sensitive and/or regulated data (e.g., organizations in the financial and healthcare industries).

For externally provisioned services (e.g., SaaS, IaaS), understand end-of-contract implications, and ask current and potential providers for an explanation of their storage reuse and recycling practices.

Business Impact: At a relatively low cost, the proper use of encryption, data sanitization and, when necessary, destruction will help minimize the risk that proprietary and regulated data will leak.

By limiting data sanitization to encryption and/or software-based wiping, organizations can preserve the asset's residual market value. The *destruction* of data-bearing devices within an IT asset typically reduces the asset's residual value to salvage, incurring the cost of environmentally compliant recycling.

The benefit rating is moderate, because data sanitization has become an increasingly accepted process to minimize the material business risk of data security. Although data sanitization will not necessarily result in increased revenue or cost savings, it will minimize the risk of significant monetary and brand damage that can result from serious ITAD-related data breaches.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Blancco Technology Group; ITRenew; WhiteCanyon Software

Recommended Reading:

"Mobile OSs and Device Security: A Comparison of Platforms"

Privacy in Japan

Analysis By: Yuichi Isoda

Definition: Privacy in Japan is regulated by the Act on Protection of Personal Information, which is supposed to be reviewed every three years. The purpose of the act is to protect the rights and interests of individuals while taking into consideration the usefulness of personal information. Another unique law worth noting is the "My Number" Law (act on the use of numbers to identify a specific individual in the administrative procedure).

Position and Adoption Speed Justification: More than 10 years have passed since the establishment of the original Act on the Protection of Personal Information. In recent years, several serious incidents raised public awareness of privacy issues and promoted a discussion of privacy in Japan. The Amended Act on Protection of Personal Information went into effect on 30 May 2017, and it contains significant changes, such as introducing rules for using personal data and adapting to globalization.

Japan became the first country to earn a reciprocal adequacy decision from the European Commission (EC) after the General Data Protection Regulation (GDPR) came into force on 25 May 2018. The adequacy decision allows personal data to flow freely between the two economies, based on strong protection guarantees on 23 January 2019.

In 2019, privacy scandals such as the Recruit Career's job seekers' disclosureoccurred in Japan. This has rekindled public debate and the law is subsequently to be amended in 2020 again. One of the key points of the reform bill is the strengthening of the subject right, which, if implemented, would further increase the maturity of privacy in Japan. In 2019 and 2020, specific privacy inquiries in digital business initiatives (e.g., Data Analytics, AI, IoT) are also on the rise. There is a growing sense that privacy is not only a matter of law, but also a matter of ethics.

User Advice: Security and risk management leaders should:

- Continue to monitor the progress of Japan's law amendment process in 2020, paying particular attention to subject rights management (see "Market Guide for Subject Rights Request Automation"), and enhance attention required for data breach detection, response and mandatory reporting.
- Incorporate a privacy assessment for the Japanese regulation in enterprise information governance by treating it as a parallel, but complementary, effort to General Data Protection Regulation (GDPR) and other privacy compliance requirements. (see "Toolkit: Assess Your Personal Data Processing Activities").
- Engage the relevant departments and tackle the issues of privacy as a matter of ethics and legal requisite in digital projects for data analytics, customer experience, AI and IoT.

Business Impact: All organizations must comply with the Amended Act on the Protection of Personal Information and the "My Number" Law. Organizations that suffer a breach of personal data will be held legally liable. An organization that mishandles personal data loses credibility not only on the legal side, but ethically as well. By complying with these regulation, and properly balancing risk and opportunity, organizations can obtain customer retention, satisfaction and reduction of brand damage risk.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Recommended Reading:

“Survey Analysis: Security Adoption and Interest in Japan, 2019-2020”

“Market Guide for Subject Rights Request Automation”

“Toolkit: Assess Your Personal Data Processing Activities”

Privacy in Russia

Analysis By: Bart Willemsen; Bernard Woo; Nader Henein

Definition: Privacy in Russia is regulated by the law on personal data, 152-FZ (27 July 2006). This law touches on all aspects of data protection — conditions for personal data processing, confidentiality, cross-border transfers, subject rights and responsibilities of the operators of personal data. In September 2015, an amendment (242-FZ) restricting the processing of personal data of Russian citizens within Russia went into effect. A second amendment (405-FZ) that significantly increased potential sanctions went into effect in December 2019.

Position and Adoption Speed Justification: The new amendment (405-FZ) not only increased potential sanctions for organizations, it introduced potential sanctions against top executives of violating companies. In addition, sanctions can increase for subsequent violations for organizations and their executives.

The enforcement of the privacy legislation in Russia has been inconsistent. The most notable sanctions to date have been a ban of LinkedIn and certain instant-messaging platforms, for violation of data localization requirements. Subsequently, both Facebook and Twitter received fines of 3,000 rubles (approximately $40) and notification of a potential nine-month ban should they fail to comply. After strengthening of the regulator’s position (Roskomnadzor) with the 2019 amendment, Facebook was fined another 4 million rubles (approximately $54,000) in 2020 for similar violations. Despite the ban, LinkedIn and other blocked resources (such as Telegram) are still popular and easily accessed with the use of VPN proxy aid.

Overall, the limited amount of regulatory enforcement activities, as well as general poor privacy awareness among customers and local organizations mean implementation of privacy practices is under development.

User Advice: Security and risk management (SRM) leaders with Russian and multinational organizations operating in Russia should:

- Examine the Russian market to identify suitable hosting providers, either cloud or data center services. Cross-border transfers must be assessed for compliance with Russian law and SRM leaders should consider usage of tools that provide anonymization techniques or data residency “as a service” for additional protection.
- Develop a data management strategy that both respects Russia’s residency requirements as well as organizational policy and standards.

- Guide discussions with executives and business stakeholders to develop a plan for maintaining communication with local regulators for awareness of shifts in approach that may necessitate adjustments in compliance activities.
- Make decisions to continue operating in Russia — including the manner of operation — based on a risk assessment of cost and benefit.

Business Impact: The majority of organizations operating in Russia have struck a balance when dealing with data protection regulations. However, such organizations should review their compliance efforts to determine if adjustments are required in light of the increase in potential sanctions.

Availability of the appropriate infrastructure facilities may also impact activities, especially for large multinational companies operating in Russia. Broad penetration of cloud services worldwide coupled with the absence in country of global players such as Amazon Web Services, Google and Microsoft provides limited opportunities for organizations with large and complicated infrastructure. Inconsistent adherence and enforcement reduce the impact to "moderate" in 2020.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Recommended Reading:

"Practical Privacy: Four Fundamental Use Cases for International Data Transfers"

"Practical Privacy — Discovery Automation of Privacy Risk"

"Toolkit: Assess Your Personal Data Processing Activities"

Secure Instant Communications

Analysis By: Dionisio Zumerle

Definition: Secure instant communications provide confidentiality and data retention for instantaneous forms of communication such as instant messaging, text messaging, voice and video communications. The solutions support smartphones, tablets and personal computers.

Position and Adoption Speed Justification: Most solutions are implemented as apps installed on a device and use encryption over the data channel. Some solutions increase their security assurance by adding a hardware-based root of trust. This can be the secure enclave or trusted execution environment (TEE) natively available on mobile devices, or a microSD card. Some solutions are instead part of stand-alone hardened smartphones. The solutions provide encryption of both the exchanges in transit and the communications stored in the device.

Secure instant communications solutions have matured along with the underlying mobile operating systems on which they operate and are able to deliver acceptable network performance, battery consumption, and efficiency in key management and encryption. User experience is the main aspect on which these solutions are trying to improve, to compete with mainstream enterprise communications solutions.

Revelations about pervasive surveillance and privacy-invasive apps have led enterprises to be concerned about confidentiality of their information. In some industries, regulations — such as the Health Insurance Portability and Accountability Act (HIPAA) and the regulations issued by the Financial Industry Regulatory Authority (FINRA) — encourage or require protection, auditing and archiving of communications. Still, adoption is limited to fulfilling regulatory obligations, or mitigating particularly sensitive scenarios.

Data retention is an increasingly important feature, as it enables monitoring and archiving for regulatory compliance purposes, and instant deletion for security assurance. Some solutions are delivered as part of broader archiving suites, and are starting to extend archiving to third-party instant messaging apps, such as WeChat and WhatsApp.

User Advice: For most organizations, the security provided by commercial enterprise communications solutions, such as unified communications, is enough to meet their confidentiality requirements. However, some organizations with high-security requirements will need a specialized, hardened instant communications solution. Typically, these are organizations at risk of industrial espionage or state-sponsored attacks and will deploy the solution to a restricted pocket of the user population that needs the solution (e.g., high-level executives). With the surge in remote work in 2020, there is a mild increase in these use cases.

Enterprises in regulated industries such as healthcare, finance, government and energy are typical adopters of secure instant communications solutions for compliance purposes. Increasingly this functionality is provided by more suitable options for the long term, namely enterprise information archiving vendors and industry-specific suites, such as clinical communication and collaboration platforms, and equivalent financial services solutions.

Software-only solutions in the form of an application are the easiest to deploy and run. While hardware-based solutions offer better performance, they impact user experience and are limited to well-defined use cases with strict security requirements.

It is not advised to rely on free consumer-grade instant communications apps that claim to offer end-to-end encryption. In addition to the lack of enterprise-grade features, these solutions are rarely a defensible choice in the event of a security incident.

Business Impact: Secure instant communications solutions protect organizations against leaks of sensitive information, and can address risks of the interception of communications in cases of industrial espionage and/or hacktivism. When used for compliance purposes, they can satisfy regulatory requirements that would otherwise have led to penalties. Outside regulated verticals and organizations with high-security requirements, mainstream organizations favor user experience and hence, when they do not use consumer solutions, they select general-purpose UC solutions or broader industry-oriented suites that include secure instant communications functionality.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Adeya; BlackBerry; CellTrust; KoolSpan; SafeGuard Cyber; Smarsh; TeleMessage; TigerConnect; Virtual Solution; Wickr

Recommended Reading:

"Market Guide for Instant Communications Security and Compliance"

"Take These Four Steps to Securely Use WhatsApp, WeChat and Other Instant Communication Apps"

"Advance and Improve Your Mobile Security Strategy"

Privacy in the EU

Analysis By: Bart Willemsen

Definition: The EU has since 2018 consolidated the privacy legislation for all member states in the uniformly applicable General Data Protection Regulation (GDPR). The GDPR applies to organizations that collect and process personal data on people in the European Union. The law replaced the Data Protection Directive 95/46/EC, which was implemented considerably different across the member states. Members of the European Economic Area (EEA) have adopted the same, and many of the principles have found follow through in various jurisdictions across the globe.

Position and Adoption Speed Justification: The GDPR is in effect as of May 2018. Hype around this new law originally peaked at YE15, but organizations globally mainly started paying attention in 2017 and 2018. The impact of the Regulation supersedes previous privacy laws that were based on the Directive of '95 in very different ways across the EU. Foundational elements include definition expansion (e.g., "processing" data, what is "personal data"), detailed provisions on accountability, risk-based approach, Privacy by Design [PbD], uniform privacy rights, and specific responsibilities for data processors. Compliance maturity levels are increasing since and a steady number of regulatory actions on different focus areas has shown the mature posture of the Regulation, as a result of decades of fine-tuning. The well-established, principle-based privacy practices are inspiring other jurisdictions to similar evolutions.

User Advice: The Regulation covers all aspects of processing personal data. Continued focus points include:

- **Data breach prevention, detection and response.** Data breaches must be reported to regulators and impacted individuals within 72 hours. Although experiencing a breach may not be sanctionable in itself, it is ultimately the key moment where adequate protection and control

over personal data throughout the data life cycle is demonstrated, or not. SRM leaders must establish an incident response team and practice playbook scenarios frequently.

- **A frictionless Privacy UX; especially regarding management of consent, preferences and subject's rights requests.** Requirements for the collection and revocation of a subject's consent are tight and individuals are empowered to a level unsurpassed. Opt-in becomes the default requirement with clear, freely-given, well-informed and unambiguous consent. Proper consent management and rights (such as to access, correction, data portability, erasure and "not to be subject to automated decisions") impact the data processing architecture and customer experience.
- **Implement Privacy by Design and by default. "**By Design" is described in another Hype Cycle entry. "Privacy by default" means that technical and organizational measures are taken to ensure that, by default, only data that is necessary for the specific, predefined and documented processing purpose is processed. Measures must be applied following a frequently revisited PIA- privacy impact assessment.
- **Get ready for certification and standardization.** International data transfers, especially outside of the EEA, may benefit from Privacy Shield self-certification (EU<->U.S. transfers), standard contractual clauses, and binding corporate rules. Industry associations can also establish codes of conduct (such as cloud service providers have done). Finally, emerging standards and frameworks such as by NIST, ISO and EuroPriSe help facilitate a standardized approach to privacy. We expect that, within two years, options will be available for obtaining more-solid certification demonstrating GDPR compliance.

Business Impact: After two years, sanctions and rulings with precedence have been passed. Focus areas here are broad and show that enforcement is gaining consistency. Regulators have started to align their interpretations and sanction level guidance. The installment of independent data protection officers (DPOs) changes reporting and corporate governance structures. Increased focus on the privacy UX requires system changes (also in backup and third-party environments), creating additional costs. The need to implement PbD demands training for application developers. Gartner has observed an increasing annual budget allocation for privacy.

On the benefit side, companies will enjoy more efficient operations based on a unified set of European privacy laws (rather than dozens of different ones) and a set of requirements that is more adapted to both the customers' expectations for privacy and to modern technologies, such as cloud computing, mobile devices, big data and social media. On a global level, the GDPR has set off many changes in other jurisdictions with maturing privacy laws. As such, "GDPR-ready" organizations will find international market access easier. Also, they will be able to capitalize on their due diligence with end users who are now more inclined than ever to choose commercial relations with organizations that better handle their personal data.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Recommended Reading:

"Toolkit: Assess Your Personal Data Processing Activities"

"Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

"5 Areas Where AI Will Turbocharge Privacy Readiness"

"Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy"

"Market Guide for Consent and Preference Management"

"Market Guide for Subject Rights Request Automation"

E-Discovery Software

Analysis By: Michael Hoeck

Definition: E-discovery software facilitates the identification, collection, preservation, processing, review, analysis and production of electronically stored information (ESI) to meet the mandates imposed by common-law requirements for discovery. These demands may be due to civil or criminal litigation, regulatory oversight or corporate proceedings. The Electronic Discovery Reference Model (EDRM) maps traditional common-law discovery into a six-step, nine-process framework for technology.

Position and Adoption Speed Justification: Market maturity and adoption vary depending on the industry and size of the organization. In highly regulated and litigious markets, e-discovery is a required practice. Use cases include litigation, Freedom of Information Act (FOIA) and other public records requests, privacy regulations, such as California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), and administrative, regulatory and post-data-breach investigations.

Data growth, expanding use cases and maturing privacy legislation are key factors in expanding e-discovery technology adoption. Adoption of Office 365 and its platform e-discovery capabilities has heightened awareness across a broader set of markets. Data growth and risk control have pushed organizations to improve the data analysis, insight and management of their information, increasing the need to automate their e-discovery process as much as possible. A mix of globalization, data sovereignty and information in the cloud is complicating e-discovery practices, shifting to more proactive, rather than reactive use cases.

User Advice: Form an information governance strategy to create a more proactive data management position and incorporate e-discovery as a part of this process, rather than an ad hoc project approach. IT should work together with the legal and compliance departments, with shared responsibility for information governance, data privacy and security issues. IT can certainly lead and shepherd the process; however, legal and compliance must identify any applicable laws and regulations as a starting point and coordinate with IT to enforce applicable policies to address these

and other general risk factors. Create deliverables ensuring that compliance and legal requirements will be met, especially planning for on-premises-to-SaaS migrations like Office 365.

The legal and IT departments must coordinate suspending the routine deletion of data and managing legal holds. These actions should be taken to make the process defensible and auditable, rather than treating each legal hold in isolation.

Enterprises should separate operational areas like collection, legal hold and infrastructure requirements from more end-user (e.g., legal, compliance) capabilities like analytics, early case assessment and document review, and weight requirements accordingly. Gartner continually sees best-of-breed e-discovery strategies, where application features/functions, user interfaces and similar characteristics drive purchasing decisions.

Additionally, e-discovery software is proving useful in other areas of enterprise data management, such as finding sensitive data and separating redundant, outdated and trivial (ROT) data from data that is business-critical, current or has been deemed a business record.

Business Impact: Major enterprises undergo dozens, sometimes even hundreds, of e-discovery cases each year. Software that supports the ability to effectively conduct and manage discovery activities not only saves time and cost, but also enables enterprises to have higher levels of confidence over risk control and compliance. End-to-end and SaaS-based solutions have accelerated adoption of bringing e-discovery inside an organization, yet many highly litigious organizations choose to employ a hybrid strategy. This can be accomplished by managing some e-discovery internally and using service providers for more complex matters.

The most important considerations are specifying a defensible and repeatable best-practice data preservation process. Enterprises that proactively plan and budget for and adopt e-discovery technologies will be less likely to disrupt and negatively impact business activities. Lastly, e-discovery practices can also be more proactive by implementing several components found within information governance plans, as well as anticipating increased global privacy and regulatory compliance requirements.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: AccessData; DISCO; Everlaw; Exterro; Logikcull; Nuix; OpenText; Relativity; Zapproved; ZyLAB

Recommended Reading:

“Market Guide for E-Discovery Solutions”

“Make E-Discovery Stronger Through Information Governance”

“Defining Your E-Discovery Process Will Lower Costs and Reduce Risks”

"Beyond GDPR: Five Technologies to Borrow From Security to Operationalize Privacy"

Privacy in South Korea

Analysis By: Elizabeth Kim

Definition: South Korea's personal data protection laws consists namely of the Personal Information Protection Act (PIPA) as a general law which prescribes how personal data is processed and aims to prevent unauthorized collection, use and disclosure of personal data. In addition to PIPA, there are several sector-specific privacy laws.

Position and Adoption Speed Justification: South Korea has continued its efforts to determine whether the current privacy regulation is sufficient in scope and enforcement. Adequacy talks between the European Commission and South Korea are still ongoing. However, several key amendments to South Korea's privacy laws (including PIPA, Network Act and Credit Information Act) will take effect per August 2020 to facilitate the adequacy decision by EU's GDPR. Additionally, these amendments will reduce redundancies caused by overlapping privacy regulations, and support "data economy" through including guidance on the use of pseudonymized data.

Personal Information Protection Commission (PIPC) will be the central administrative agency with supervisory authority for data breaches replacing the current structure where the responsibility was across the Ministry of the Interior and Safety (MOIS) and the Korea Communications Commission (KCC), both of which are government entities.

Based on South Korea's significant steps to refine its privacy laws and the increased regulatory enforcement, the maturity has moved further into the Slope of Enlightenment. However, we cannot discount recent concerns that were raised about personal privacy that needs to be addressed:

- Social issues such as the Nth Room case scandal posing the question on how to account for the people's misuse of their right to privacy in criminal activities.
- COVID-19 creating concerns around preserving one's right to privacy against the government's response to the pandemic.

User Advice: To facilitate compliance with South Korean privacy regulations, privacy officers of organizations processing personal data of South Korean customers should determine applicability of PIPA and the various sectoral laws including but not limited to:

- Act on the Promotion of Information and Communications Network Utilization and Information Protection (often referred to as Network Act or ICNA)
- Use and Protection of Credit Information Act (often referred to as Credit Information Act)
- Act on Real Name Financial Transactions and Guarantee of Secrecy
- Electronic Financial Transactions Act
- Act on the Protection and Use of Location Information

Compliance assessment should be performed against these applicable privacy laws as well as ongoing monitoring of any updates and revision of guidelines, paying specific attention to the main changes in PIPA, which can be summarized as the provision of clearer distinction between personal data, pseudonymized data and anonymized data. Furthermore, under the amended PIPA, data handlers may process pseudonymized data without the consent of the data subject for purposes of statistical compilation, scientific research, and record keeping purposes for the public interest.

It is also important to have a good understanding of the EU GDPR given that recent updates and future changes to PIPA will closely align to many aspects of GDPR as the effect of South Korea's ongoing effort to qualify for the adequacy decision.

Business Impact: The business impact of PIPA is significant due its comprehensive application and the potential penalties resulting from noncompliance, which include regulatory fines and criminal sanctions. In fact, there was a recently reported case where a privacy officer was held personally liable and fined 10 million South Korean Won (approximately $8,600) for a data breach and for noncompliance with PIPA and the Network Act. This was in addition to the fine of 327 million South Korean Won (around $280,000) imposed against the company. There are two similar cases pending where personal liability is imposed on the privacy officers. It can be argued that the significance of these cases is not in the amount of the penalty, but that the privacy officer was held personally accountable, which will set precedence for future cases of data breaches. Since the introduction of PIPA, majority of companies doing business in South Korea seem to have found appropriate mechanisms for dealing with the law. However, with the increased enforcement and several significant updates to the privacy laws, organizations will need to closely monitor developments and continue to assess their compliance against PIPA and related sectoral laws.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Privacy in the U.S.

Analysis By: Nader Henein; Katell Thielemann

Definition: Privacy laws in the U.S. protect personal data and the privacy of individuals and, in certain cases, require disclosures and notifications to affected parties. U.S. privacy laws are currently overwhelmingly state-specific (with notable sector-specific examples in government, healthcare, education and financial services).

Position and Adoption Speed Justification: Over the course of 2019 and early 2020, three state privacy laws went into effect: California (AB 375), Nevada (SB 220) and Texas (HB 4390). The California Consumer Privacy Act (CCPA) was the most far-reaching, setting the stage for how organizations across all 50 states looked at structuring their privacy programs and prepared for compliance. At the federal level, efforts continue to falter with state law preemption and enforcement mechanisms representing major sticking points.

Other notable recent state-level developments include Washington's new facial recognition law, which treats government use of facial recognition technology as a very significant privacy issue and imposes extensive requirements and limitations on government use. In addition, a flurry of lawsuits under Illinois' Biometrics Information Privacy Act (BIPA) have been filed in 2019, and the $550 million settlement by Facebook in January 2020 will likely spur more.

The landscape will continue to fragment with each state law, and while movement is occurring, the lack of a unified U.S.-wide approach means this topic will continue to occupy boardrooms.

User Advice: Even with COVID-19 looming over our heads and multiple pleas made to the California attorney general to postpone CCPA enforcement (currently set for July 2020), the deadlines seem to stay on track. The best advice continues to be alignment with the most far-reaching current U.S. law and, as it stands, this continues to be the CCPA. More state laws are expected across 2020, and some may be more stringent. To facilitate compliance with such a disparate array of privacy obligations, many organizations with international reach are choosing to adopt the EU GDPR as their global default. Focus should be on the important underlying privacy management program elements with broadest benefit (for example, data mapping, cost allocation of request management), instead of compliance-oriented efforts.

In the face of mounting complexity, privacy, security and risk management leaders should also partner with their legal counsel to understand which vertical industry laws apply to them, their regulatory obligations and the specific privacy (and security) practices these laws mandate. Examples include:

- The Privacy Act (specifically as part of federal assistance under the Coronavirus Aid, Relief, and Economic Security [CARES] Act)
- HIPAA/HITECH/HITRUST in healthcare
- The Family Educational Rights and Privacy Act (FERPA)
- The Gramm-Leach-Bliley Act (GLBA) for financial institutions
- The Fair Credit Reporting Act (FCRA)
- The Children's Online Privacy Protection Act (COPPA)
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) of 2003
- The Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018

Business Impact: The business impact of not complying with U.S. privacy laws varies. Depending on the industry, the state and the specific law, this can include fines of more than $10 million, 20 years of imposed third-party privacy audits, loss of business license, substantial reputational damage or class-action lawsuits. A privacy violation could also be an administrative offense that goes unnoticed. Personal sensitivities to privacy issues have markedly increased in 2018, and more organizations are turning to privacy programs as positive business efforts rather than mere

compliance burdens. Qualified legal advice is necessary to determine the business impact in any given state and sector.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Recommended Reading:

"The State of Privacy and Personal Data Protection, 2019-2020"

"How to Prepare for the CCPA and Navigate Consumer Privacy Rights"

"Toolkit: Assess Your Personal Data Processing Activities"

"Toolkit: Security Incident Response Roundtable Scenario for Privacy"

IT Risk Management Solutions

Analysis By: Khushbu Pratap; Claude Mandy; Brent Predovich

Definition: IT risk management (ITRM) solutions operationalize the risk management life cycle for scenarios originating in or attributed to digital infrastructure, applications, systems, processes and teams. These deliver primarily three ITRM buyer use cases: basic risk and controls self-assessment, advanced risk management and governance, and cybersecurity risk management. ITRM solutions have Critical Capabilities ranging from workflow design, risk analysis and reporting, to board reporting, digital asset discovery, and basic and advanced integrations.

Position and Adoption Speed Justification: The ITRM market maturity level continues at "early mainstream," with a market penetration of 20% to 50%. It is not projected to plateau for another three to five years. The pandemic has shined a strong light on IT operational dependencies, even more so as a result of moving to remote and extended operating environments. Combined with a continuing, heightened focus on cyber-risk exposures, buyers have maintained high levels of interest in ITRM solutions; and interest will persist due to cybersecurity mandates seen worldwide. Although many organizations are using ITRM solutions to manage security and technology risk exclusively, they have begun adding business context in prioritizing vulnerabilities. This prioritization of business context aligns with a steadily increasing maturity in risk management discipline. Adoption levels for ITRM solutions have been higher in North America and Europe, followed closely by the APAC region. We see slow adoption in the Middle East and Africa.

User Advice: Gartner discourages buyers from trying to use these solutions to create functions and workflows without process clarity in their organizations. The market reality is that not all buyers wait for sufficient maturity of their processes before looking to automate those processes and, by doing so, often cause more confusion and loss of time and investment. There is no single best product for all organizations. However, there are typically several good options to fit a specific set of requirements. Key considerations in planning and procuring ITRM solutions include the following:

- Use Gartner's definition of ITRM solutions as a starting point and tailor to your requirements. Go beyond capabilities, implementation, integration, price and support. Select vendors based on their ability to scale and flex with your risk management journey.
- Organizations looking to deploy ITRM solutions must know that the labor associated with populating asset, process, risk and control repositories is significant. This should be considered prework in operationalizing ITRM as an initiative. The scope of prework varies for organizations and, at minimum, requires one FTE.
- Buyer interest in ITRM solutions is often combined with interest in vendor risk, corporate compliance, operational risk or audit management solutions. The main advantage is integration of risk data, workflow and dashboards served up consistently with context to risk owners, risk management teams, and internal audit respectively. If there is no need for correlated information all in one place, then a best-of-breed vendor in one of these areas may be a better choice.

Business Impact: ITRM solutions can offer tangible, direct cost savings in replacing manual effort of FTEs that are needed to coordinate and evidence risk governance in the digital environment. For heavily regulated organizations, penalties avoided from industry enforcement bodies and regulators are attributed toward indirect savings. For all organizations, operational disruptions avoided by potential incidents traced to digital infrastructure, services and applications can be attributed to the cost of running resilient organizations.

Among intangible benefits, ITRM solutions track deviations against chosen baselines and facilitate monitoring of selected risk indicators. Approximately 30% buyers globally either plan to consolidate information in ITRM solutions or already do so to enable management of cyber-risk initiatives. This facilitates cyber-risk reporting to senior management and board members directly or by way of rolling up risk to enterprise risk dashboards and supporting internal and external audits.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Allgress; Dell Technologies; Galvanize; IBM; LogicManager; MetricStream; NAVEX Global; Resolver; SAI Global; ServiceNow

Recommended Reading:

"Critical Capabilities for IT Risk Management Solutions"

"Critical Capabilities for IT Vendor Risk Management Tools"

"6 Principles for Digital Business Risk Assessment"

Cloud Access Security Brokers

Analysis By: Steve Riley

Definition: Cloud access security brokers (CASBs) provide crucial cloud governance controls for visibility, data security, threat protection, and compliance assessment in SaaS and IaaS. CASBs consolidate multiple types of security policy enforcement into one place. Examples include authentication, single sign-on, authorization, device profiling, data security, logging, alerting, and malware removal. Most CASB deployments are cloud-based; on-premises deployments are rare.

Position and Adoption Speed Justification: Vendors offer feature-rich products to increase cloud visibility and apply consistent policy across multiple providers. Execution across all vendors is variable: while some have incrementally improved and added new capabilities, the leading vendors continue to make significant investments that have contributed to the rapid maturation of the market. The acquisition phase of the market has ceased. Major incumbent security vendors now offer a CASB, either stand-alone or as part of a product portfolio; integration with other products in portfolios is inconsistent but improving. While the number of independent vendors has stabilized, the most relevant independent vendors demonstrate sustained innovation and broad market reach. Differentiation among vendors is becoming difficult, and several have branched beyond SaaS governance and protection to include custom application support in IaaS clouds, cloud security posture management (CSPM) capabilities, and user and entity behavior analysis (UEBA) features.

The most relevant independent vendors continue to receive venture capital funding, while funding for the less well-known private vendors remains uncertain. The pace of client inquiry indicates that CASB is a popular choice for cloud-using organizations. Gartner's 4Q19 security spend forecast predicts a significant but slowing growth rate for CASB: 45.3% in 2020, 40.7% in 2021, 36.7% in 2022, and 33.2% in 2023. While the forecast predicts slowing spend for all security markets, CASB's growth remains higher than any other information security market (see "Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 4Q19 Update").

User Advice: Examine vendor capabilities in four functionality areas: visibility, data protection, threat detection and compliance. All relevant CASB vendors interact with SaaS applications via APIs and can be positioned in-line for real-time traffic visibility. CASB proxies may or may not require endpoint agents for traffic steering outside proxied networks; factor this into your evaluation. Increasingly, CASB vendors offer remote browser isolation as an adjunct to in-line deployments.

Common deployment scenarios that deserve special scrutiny include:

- **Cloud discovery and risk assessment.** Evaluate the thoroughness of the CASB's analysis of an organization's cloud security posture. The CASB should discover every cloud service in use and assign each one a risk score (ask vendors for information about how often this is updated), gleaned from attributes whose weights can be modified by customers. Evaluate the CASB's CSPM capabilities for assessing risk in IaaS storage, compute, and virtual network configurations.
- **DLP.** Evaluate whether CASB capabilities are sufficient or require augmentation with deployed enterprise DLP product, either via ICAP or RESTful API integration. In-line CASB DLP capabilities should provide a mechanism to control the movement of sensitive information into and out of cloud services in real time. Examine CASB support for data classification features that can link to existing enterprise classification tools.

- **Adaptive access control (AAC).** Examine techniques vendors provide for altering the behavior of governed applications based on signals observed during and after login. AAC allows for shades of access (e.g., read-only access to content on unmanaged devices) that are more useful to the business than blocking access completely.
- **UEBA.** Evaluate how CASBs detect and isolate risky users and devices. Insider threats and compromised accounts are common attack vectors. Seek mechanisms that build baseline behavior profiles (such as typical upload/download amounts and user locations) and alert and mitigate when behavior deviates from baselines. Step-up authentication is an important capability to test with whatever IAM vendor is already deployed.
- **Third-party app discovery and control.** Ensure that the CASB can detect all third-party apps that have been granted access to SaaS applications (almost always via OAuth). Look for more than single yes/no controls for each app and instead favor the ability to group third-party apps into categories based on OAuth scopes.
- **Regulatory compliance.** Determine whether the CASB offers sufficient visibility and control for aspects such as user privacy and data residency. Carefully scrutinize encryption mechanisms. Encrypting data before sending it to a cloud service might negatively affect certain functionality in the service. Evaluate the CASB's CSPM capabilities for comparing IaaS workload configurations to common regulatory baselines.

Business Impact: CASBs are uniquely positioned to enable organizations to achieve consistent security policies and governance across many cloud services. Unlike traditional security products, CASBs are designed to protect data that's stored in someone else's systems. CASBs are suitable for organizations of all sizes in all industries and are uniquely positioned to help demonstrate that cloud use is well-governed. Given the expected continued feature expansion and relative ease of switching, favor one-year contract terms over lengthier ones.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Bitglass; Censornet; CipherCloud; Forcepoint; McAfee; Microsoft; Netskope; Proofpoint; Symantec; Zscaler

Recommended Reading:

"Magic Quadrant for Cloud Access Security Brokers"

"Critical Capabilities for Cloud Access Security Brokers"

"Peer Lessons Learned: Implementing Cloud Access Security Brokers"

"How to Secure Cloud Applications Using Cloud Access Security Brokers"

"Best Practices for Planning, Selecting, Deploying and Operating a CASB"

Dynamic Data Masking

Analysis By: Dale Gardner

Definition: The goal of dynamic data masking is to mask data in real time, as it is accessed. DDM changes the data stream as part of processing a request, so that the requester is not given access to the real, sensitive data. It does not protect the original data at the storage level.

Position and Adoption Speed Justification: The growth of dynamic data masking (DDM) continues to be driven by evolving compliance and threat landscapes, as well as its relative ease of implementation. DDM adds a configurable layer of security, with minimal to no modifications to existing applications.

Traditionally, DDM solutions have intercepted queries and responses at the database layer, with some solutions operating at the application layer; however, the technology is increasingly being used in new channels — notably API gateways and data virtualization. Database vendors are also increasingly supporting DDM natively (e.g., Oracle, Microsoft and SAP).

The continuing impact of privacy regulatory requirements led by the General Data Protection Regulation (GDPR), the growth in deployment options and the increasing availability of DDM as a feature will accelerate adoption. DDM is also attracting a great deal of interest with the growth of big data projects, in which the aggregation of sensitive data can lead to complex compliance and security concerns. However, DDM does not address data residency concerns, which may limit its growth.

Gartner expects DDM to reach the Plateau of Productivity during the next two years.

User Advice: We recommend the following:

- Consider DDM in combination with attribute-based access control (ABAC), database audit and protection (DAP), format-preserving encryption (FPE) and tokenization for the protection of sensitive data in applications and in storage.
- Use DDM to address masking requirements in production environments, or environments in which the organizations cannot make changes to the data in the underlying database, and data-at-rest protection is covered by other means. Common use cases for DDM include masking customer data for call center applications and preventing sensitive data access by database administrators (DBAs).
- Assess the suitability of solutions against the specific, targeted portfolio of applications and target use cases as part of the DDM tool selection process. Consider proofs of concept (POCs) that include performance impact. Some applications are not as easy to modify as others using DDM. Application database service accounts and database connection pooling can prevent DDM from understanding the actual user or service accessing the data.
- Look at your overall data protection needs. There are synergies among DDM, DAP, tokenization and encryption, and some vendors are offering combinations of these capabilities in a single tool. Many DDM vendors also have static data masking (SDM) offerings, but not all of them do.

Business Impact: Adopting DDM helps organizations address evolving compliance and threat landscapes by minimizing exposure to sensitive data, without extensively modifying existing applications. It can provide an agile and cost-effective way to address such new requirements.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Dataguise; DataSunrise; IBM; Informatica; Mentis Technology; Microsoft; Oracle; Privitar; SAP; SecuPi

Recommended Reading:

"Market Guide for Data Masking"

"Creating a Data Strategy"

"Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization"

Cloud Application Discovery

Analysis By: Jay Heiser

Definition: Cloud application discovery (CAD) refers to mechanisms for security, licensing, compliance and I&O professionals, providing visibility into enterprise activity associated with the use of public cloud applications. CAD provides information on application name and type, and usage by individual and department. Ideally, an application discovery tool also provides information about the cloud service provider, including a risk rating.

Position and Adoption Speed Justification: IT professionals are increasingly recognizing that the identification and analysis of unsanctioned IT are critical elements of data governance, cybersecurity and IT spend management, encouraging the utilization of CAD functionality. Regulations, especially the EU GDPR and CCPA, are providing additional incentive to determine what SaaS applications are being used in what way. Dozens of multifunction products offer different levels of CAD functionality, supporting different corporate IT roles. CAD is not a stand-alone market, but rather a feature of several categories of multifunction management tools. It is a primary capability of cloud access security broker tools and SaaS management platforms, and a secondary capability of software asset management, DNS solutions, firewalls and secure web gateway products. The proliferation of CAD across so many different functions represents a confusing market, but it means that most IT departments already have some capability to identify "shadow IT," although many have not yet tried to apply this capability.

User Advice: All organizations that are heavily regulated or have large amounts of critical data should be either controlling access to SaaS or monitoring SaaS usage through CAD mechanisms. As more enterprises put policies in place that require explicit risk acceptance decisions for the use

of SaaS, they require mechanisms to identify unauthorized SaaS use and monitor authorized SaaS use to ensure it is meeting policies. The decision about when and where to place additional controls over the "virtual enterprise" represented by SaaS starts with tools that can report on the extent to which external applications are being utilized. This provides information in support of defensible decisions about the organizational use of SaaS, and will ensure that "unsanctioned IT" can be identified, helping organizations prioritize their SaaS risk assessment and control efforts.

CAD products differ in the sources used for collecting the data, which can come directly from the endpoints or, more conveniently, from firewalls or secure web gateways. They also differ in the level and form of information they report. The most useful CAD products provide some information that can help IT security, privacy, compliance and other IT governance functions to focus attention on the applications that are most likely to represent higher levels of risk.

Business Impact: Most organizations have hundreds, even over 1,000, SaaS applications in regular use, many of which the IT department is unaware of, and most of which are not IT's direct responsibility. Cloud discovery tools are useful in identifying this "unsanctioned IT," facilitating security, compliance, SaaS license management and even control over usage fees. Most organizations have some form of tool that includes a CAD function, but the majority of organizations still fail to fully apply this capability, thus complicating the estimate of market penetration. Gartner anticipates that visibility into cloud application usage will eventually be considered a mandatory function by auditors and regulators, but the level of urgency continues to be relatively low.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Censornet; Eracent; Flexera; McAfee; Microsoft; Netskope; Scalable Software; Snow Software; Symantec; Torii

Recommended Reading:

"Magic Quadrant for Cloud Access Security Brokers"

"How to Develop a SaaS Governance Framework"

"Solution Path for a SaaS Adoption Framework"

Privacy in Latin America

Analysis By: Bart Willemsen; Claudio Neiva

Definition: The constitutions of most of the countries in Latin America contain statements regarding the assurance of privacy, and some of these have considerably expanded or clarified the right to privacy in common national legislation. Historically, privacy in Latin America has aligned with European standards, introducing some variations, but they have consistently lacked clear implementation guidance and enforcement.

Position and Adoption Speed Justification: Latin American countries that have adopted data protection laws include Argentina, Brazil, Chile, Colombia, Panama, Paraguay, Peru and Uruguay. Argentina and Uruguay have an adequacy standing with the European Union (EU), but further modernization of their laws is expected in lieu with the European Data Protection Board's (EDPB) review of adequacy decision continuation. Uruguay has yet to take action and Argentina is working to update its privacy law to better align with the General Data Protection Regulation (GDPR).

Brazil's new LGPD, similar to the GDPR in nature, be enforceable as of August 2021. Chile is making amendments as well, including enhancement of regulating biometric and sensitive data. Additional sector and topic-specific privacy legislation is found as well, for example on e-commerce (e.g., El Salvador and Paraguay).

The observed inconsistent enforcement plays only a small part in the Hype Cycle position, especially as strengthening of privacy legislation across the countries, including Mexico and others, is expected within the next few years. As such, privacy in Latin America may see a new cycle kick-started soon.

User Advice: Commercial organizations operating in Latin America, or providing services or products to customers there, should be aware of impending and enacted regulations and constitutional provisions for privacy. In general, a privacy program that adheres to the principles of the GDPR will meet the majority of requirements of most privacy regulations in Latin American countries. Pending enhancements over the next few years of the detail of data protection requirements are likely to follow the enhanced principle-based requirements as outlined in the GDPR. Organizations should expand control and compliance efforts across the supply chain as well. In most of these jurisdictions, the onus is primarily, if not only, on the covered entity to ensure adequate data protection down to service providers and subprocessors.

Foundational elements to include in a privacy program for Latin America include the principle of purposeful processing, transparency, expansion of individual privacy rights and thus the required control over personal data throughout the data life cycle. In addition, organizations should have insight in potential cross-border data transfers. For example, Colombia has data residency requirements, and its data protection authority has a list of countries that have been identified as offering adequate levels of protection for personal data. Argentina has similar requirements for the protection of personal data. Such conditions affect multinational companies that process personal data in the cloud or in offshore data centers (such as in India and the Philippines).

Business Impact: When the LGPD comes into force, the perspective on data processing and storage will change concerning each processing purpose. IT leaders will also have to take into account jurisdiction and industry specific data residency requirements in their international transfers and cloud adoption (e.g., the Brazilian banking sector where restrictions apply). In terms of priority, SRM leaders need to:

- Map specific requirements of each country that has a business relationship for data residency and legal involvement.
- Identifies the different subject rights requests (SSR) requirements for each country. The response requirements to the individual are different compared to GDPR.

- Collaborate with the highest management on the understanding that privacy is an organizational issue and not primarily technological to gain support and adequate governance of the privacy program.
- Implement privacy impact assessments (PIA), to keep risk mitigating measures adequate to the risk assessed.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Recommended Reading:

"The Impact of Privacy on Procurement and Vendor Selection and Control"

"Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

"What You Need to Know About Privacy in LATAM"

"Toolkit: Assess Your Personal Data Processing Activities"

Entering the Plateau

Database Audit and Protection

Analysis By: Brian Lowans; Joerg Fritsch

Definition: Database audit and protection (DAP) provides centralized and consistent security across a variety of database management systems (DBMSs) for both relational and NoSQL databases. Most vendors are now expanding support for cloud-based DBMS. DAP sets and manages DBMS user privileges, monitors user behavior with data and provides database audit logs. It can detect unusual activity and send alerts to prevent a breach. DAP is a critical security control to help meet data residency and data protection and privacy compliance requirements.

Position and Adoption Speed Justification: The DAP is maturing for on-premises deployments. Its ability to control user and administrator privileges, as well as monitor user activity with data, uniquely provides prebreach, real-time breach, and forensic or incident response analytics. This user analytics with data context is not addressed by tools such as identity and access management (IAM), security information event management (SIEM), or user and entity behavior analysis (UEBA). The core DAP monitoring capabilities are maturing. Several products offer machine learning (ML) to enhance behavior analytics, identify the user account and gain deeper insight into the environment. Support for cloud-based databases, big data and NoSQL platforms (e.g., Apache Hadoop, MongoDB and Cassandra) are growing. Vendors continue to develop capabilities for algorithmic detection of malicious activity, due to hacking or insider misuse and emerging capabilities to help with monitoring and audit for privacy requirements.

User Advice: DAP provides a comprehensive, uniform and cross-platform database security suite across heterogeneous database environments. Clients should implement DAP functionality to mitigate privacy risks and data breaches resulting from user and administrator activities, database vulnerabilities, and poor segregation of duties (SOD), especially when DBMS vendors don't provide adequate capabilities to do so. DAP provides unique security functionality because it intercepts all communication paths to the database to then analyze and/or modify SQL commands and/or responses. It should be used as part of a broader, risk-based strategy by using the data security governance framework to help select and deploy complementary security products. Use DAP for five common use cases:

- **Unification of data security policies —** Do not rely on siloed and independent native database security functions. Apply and monitor unified database security policies across large-scale heterogeneous database environments to maintain data protection and privacy across geographic jurisdictions.
- **User activity monitoring —** Identify and assess the who, what, why, where, when and how of all users, including administrators and highly privileged application users. Monitor the activity of all users with data context to detect any privilege changes, as well as unusual data access and security policy violations, either accidental or malicious, that might lead to data breaches.
- **Enforcement of access controls —** Enforce the SoD of privileged and application users. If access to sensitive data is not permitted, then particular fields can, for example, be blocked or redacted. Some vendors may even be able to anonymize the field (e.g., using masking, tokenization and encryption). If privileges change, access can also be blocked until verified.
- **Attack prevention —** Identify and mitigate open vulnerabilities in each DBMS and verify configuration or schema changes to prevent malicious activity. Applies virtual patches to block SQL attacks.
- **Audit and forensic analysis and reporting —** Use the audit report to provide a full record of activity for compliance reporting. Traditional database auditing has a significant impact on performance of the database servers; however, DAP technologies collect the same amount of data (or even more), with low to negligible performance impact. This is a best practice for all data stores in scope of regulatory frameworks that require audit records and breach notification. Many regulations require notification of datasets affected. Privacy laws, such as the General Data Protection Regulation (GDPR). require detailed reporting of data breach details within 72 hours.

If not provided by the vendor, data protection tools, such as format preserving encryption (FPE), tokenization and dynamic data masking, should be used in parallel with DAP to restrict access and protect data at rest and/or in use. This allows a greater focus on and monitoring of privileged users.

Business Impact: DAP is an important addition to enterprise data security governance programs, because it provides data context against user privileges and activity; other tools, such as IAM, SIEM or UEBA, do not. It is a critical investment to protect large and/or heterogeneous database infrastructures or Hadoop deployments containing regulated or business-critical data. It is important to address typical audit recommendations, such as enforcement of segregation of duties,

vulnerability management, user activity monitoring and providing a forensic audit record of all activities. With increasing risks caused by data residency and privacy, hacking and insider abuse, DAP is a critical preventive and detective technology.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Beijing DBSec Technology; DataSunrise; IBM; Imperva; McAfee; MENTIS; Oracle; SecuPi; Trustwave; WareValley

Recommended Reading:

"Use the Data Security Governance Framework to Balance Business Needs and Risks"

"Market Guide for Data-Centric Audit and Protection"

"Securing the Data and Advanced Analytics Pipeline"

"The Future of the DBMS Market Is Cloud"

"Consuming DBaaS Securely: Comparing Options for Securing On-Premises and Cloud Databases"

Cloud Security Assessments

Analysis By: Khushbu Pratap

Definition: The buyers and sellers of public cloud services need affordable and reliable ways to assess provider security and continuity. Formal assessment are performed by independent evaluators that are authorized by an authentication body to use published control standards and process guidelines to evaluate service provider security posture, and to publicly share their findings.

Position and Adoption Speed Justification: Every globally active Tier 1 cloud service provider (CSP), such as Amazon Web Services (AWS), Box, Dropbox, Google, Microsoft, Salesforce and Workday, has completed several formal third-party security risk assessments. Approximately one-half of the growing number of Tier 2 cloud service providers have also undertaken at least one formal security assessment (although rapid growth in the number of midsize CSPs continues to make this a difficult estimation). Virtually none of the huge number of Tier 3 CSPs have undertaken a formal evaluation. Customer data from cloud access security broker vendors suggests that while less than one out of 10 CSPs have been formally evaluated, almost half of all enterprise traffic to the public cloud is flowing to assessed vendors. For this reason we consider cloud security assessments to have reached mainstream maturity.

Formal evaluation is becoming a standard for CSPs that wish to provide services to enterprise customers. Gartner anticipates that within several years, virtually all Tier 1 and Tier 2 CSPs, representing virtually all strategically significant providers, will successfully complete and maintain a cloud security assessment.

User Advice: Cloud service buyers that desire useful levels of assurance for cloud service security and reliability for the least cost and effort should use CSPs that have been verified through a standards-based, third-party evaluation. By a significant degree, ISO/IEC 27001 and SOC 2 are the two most widely recognized and available standards-based formal evaluations being used by cloud service providers. Although they are not yet widely applied, Gartner anticipates that a growing number of cloud security assessments will include evaluation of controls from the ISO/IEC 27017 cloud security standard, and the ISO/IEC 27018 cloud privacy standard. This will ensure that the assessment process addresses cloud-specific security concerns. Organizations handling credit card data must use services that have successfully undergone a Payment Card Industry Data Security Standard (PCI DSS) evaluation. And U.S. federal agencies should be using services that have undergone the Federal Risk and Authorization Management Program (FedRAMP) evaluation process. In all cases, higher levels of assurance can be attained by requesting a copy of the detailed findings report from the third-party evaluator and thoroughly reviewing it against the specific needs and risks of your use case.

If a formal third-party evaluation is not available from a service provider, then the buying organization should at least ensure in writing that the CSP is meeting a minimum expected set of controls. Ask for a complete response to one of the published cloud risk questionnaires. De facto standard templates are available from Shared Assessments, the Cloud Security Alliance and the U.S. FedRAMP program. These are constructed in the form of yes/no questions; however, in critical use cases, much more detailed risk assessment information can be obtained by replacing the binary "Do you?" with "How do you?" This approach cannot provide the level of rigor and assurance typical of a formal third-party evaluation.

Most CASB tools include a cloud application discovery capability that scores the risk relevance of cloud service providers, and several security ratings service (SRS) vendors also provide scores indicative of estimated CSP security posture. While the full accuracy of these scoring mechanisms remains an open question, they are being used by a growing number of Gartner clients to help determine the security acceptability of CSPs that have not undergone a formal third-party evaluation.

Do not automatically assume that all cloud services must meet the same security standards. Tier 3 cloud service providers are typically not being used in strategically important ways, so their lack of formal security assessment is usually acceptable.

Business Impact: The impracticality of conducting a resource-intensive manual risk assessment process has historically inhibited the cloud computing market, and it is becoming awkwardly obvious that questionnaires take too much effort to provide too little risk-relevant information. The use of formal cloud risk evaluations is proving increasingly beneficial in reducing the market friction caused by concerns over security and the current lack of transparency. Additionally, it serves as a signal to prospects that the provider intends to continue investing in security. Formal security assessments allow cloud buyers to concentrate on the functional aspects of the available services, without having to waste time in fruitless exercises to determine whether the CSP is "secure" or not.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: A-LIGN; BSI; Coalfire; EY; KPMG; PwC; Schellman

Recommended Reading:

"Inform Your Cloud Service Choice With Provider Maturity"

"Market Guide for Organization Security Certification Services"

"How to Evaluate Cloud Service Provider Security"

"FedRAMP Demystified"

Database Encryption

Analysis By: Brian Lowans

Definition: Database encryption solutions protect the column, table or database on-premises instances of relational database management systems (RDBMSs).

Position and Adoption Speed Justification: There is an increasing focus on database encryption as a risk-based access control (RBAC) by data protection and privacy laws and to address data residency issues. Encryption is growing in importance to minimize the risk of a data breach and to maintain privacy through data protection, the enforcement of segregation of duties (SOD) and access control.

User Advice: Authorized users and database administrators (DBA) with database access privileges have access to all data, unless encryption is used as a blunt-force data access control. Organizations should use the data security governance (DSG) framework to decide whether to implement encryption at the database, column or field level. They should also consider complementary tools to monitor and audit all user and DBA access to sensitive data with database audit and protection (DAP) tools. Although several RDBMS vendors are offering native transparent database encryption (TDE) capabilities (at the database, table or column), these are unique to that platform, with localized key management. They are typically managed by the DBA. Database encryption vendor products, however, apply security policies across multiple RDBMS platforms with a centralized enterprise key management (EKM). DBAs should not have management responsibility for encryption, but EKM will provide consistent security policies across the different RDBMS platforms. When considering database encryption, conduct a careful assessment to identify:

- What data needs to be protected, based on perceived risks, threats and compliance requirements?
- What is the overall data security policy?
- Should encryption be combined with DAP?

- How will SOD and access control be handled?
- Should encryption be applied to protect the whole database instance, the tablespace, or individual columns or fields?
- If protecting columns, is format-preserving encryption (FPE), tokenization and dynamic data masking (DDM) needed?
- How will the chosen database encryption integrate with an EKM strategy?

Most deployments focus on anonymization of specific types of regulated data — such as credit card numbers, personally identifiable information (PII), protected health information (PHI) and financial data. Mature users then branch out using risk-based approaches to include critical, but nonregulated data. Evaluate any impact on performance and functionality of applications accessing the RDBMS, and be aware that other security and database functionality, such as data discovery, can be affected.

Business Impact: When implemented consistently and aligned with the correct risks, database encryption, can offer a strong level of control against unauthorized access to data. It is a blunt-force tool that limits access to specific user accounts. However, more comprehensive security can be provided if combined with other tools, such as DAP. Consequently, concerns about the privacy of PII and PHI, data breach disclosure regulations, and the PCI Data Security Standard (DSS) are putting pressure on organizations to make greater use of encryption. Data residency across borders is also driving the need for additional anonymization options to protect data in use. Consider combining or replacing TDE with field protection methods such as FPE, tokenization or DDM to enforce stronger SOD. RDBMS encryption is increasingly recommended by auditors, but may not specify which method is required. Organizations need to use the DSG framework to review how other compensating security controls can be implemented as part of a broader, data-centric security strategy.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: eperi; IBM; Micro Focus; NetLib; Oracle; Penta Security Systems; PKWARE; Protegrity; Thales eSecurity; Townsend Security

Recommended Reading:

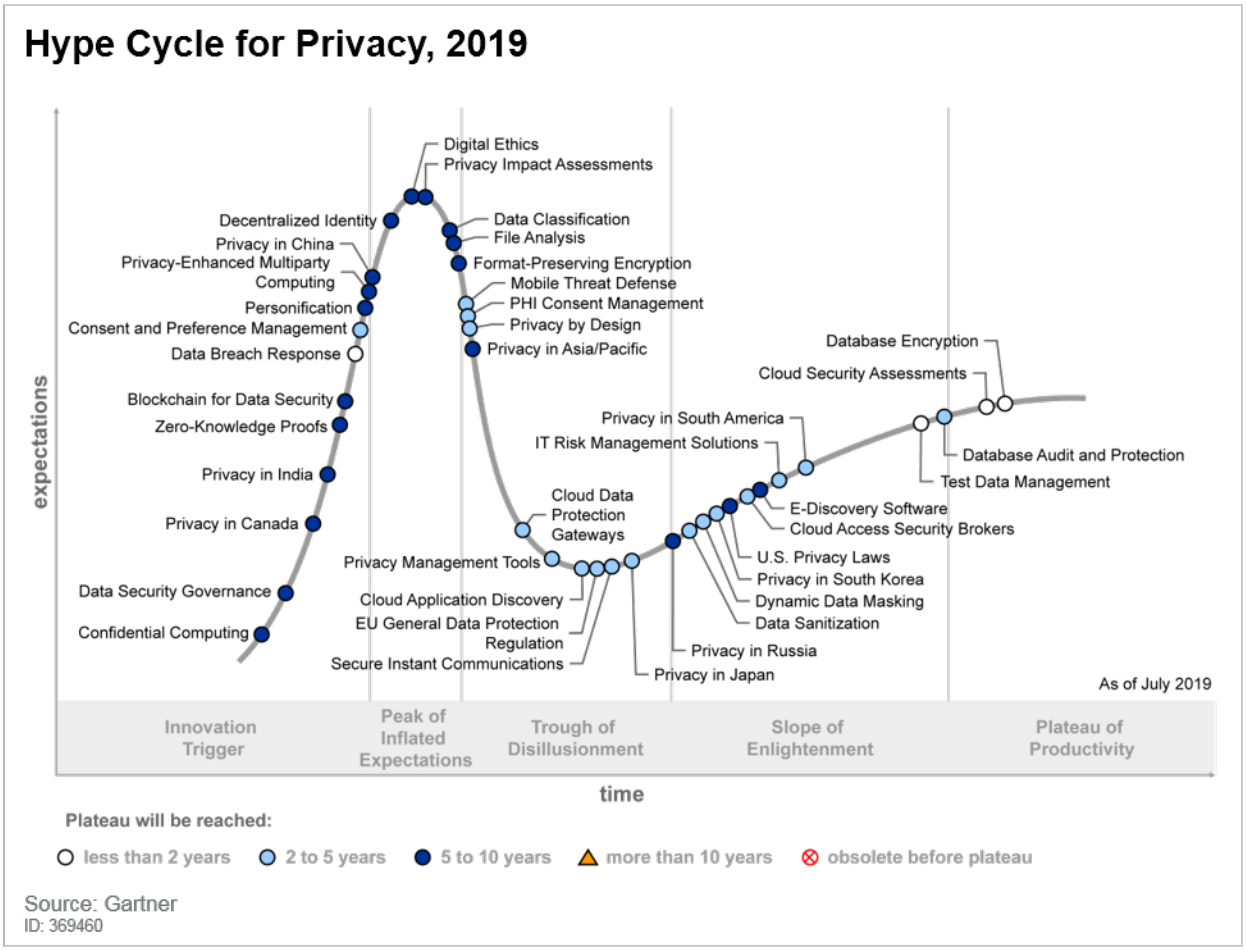
“Use the Data Security Governance Framework to Balance Business Needs and Risks”

“Develop an Enterprisewide Encryption Key Management Strategy or Lose the Data”

“Prioritize Enterprisewide Encryption for Critical Datasets”

Appendixes

Figure 3. Hype Cycle for Privacy, 2019



Source: Gartner
ID: 369460

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant press and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology's applicability, risks and benefits. Commercial off-the-shelf (COTS) methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the technology to reach the Plateau of Productivity.

Source: Gartner (July 2020)

Table 2. Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2020)

Table 3. Maturity Levels

Maturity Level	Status	Products/Vendors
Embryonic	■ In labs	■ None
Emerging	■ Commercialization by vendors ■ Pilots and deployments by industry leaders	■ First generation ■ High price ■ Much customization
Adolescent	■ Maturing technology capabilities and process understanding ■ Uptake beyond early adopters	■ Second generation ■ Less customization
Early mainstream	■ Proven technology ■ Vendors, technology and adoption rapidly evolving	■ Third generation ■ More out-of-the-box methodologies
Mature mainstream	■ Robust technology ■ Not much evolution in vendors or technology	■ Several dominant vendors
Legacy	■ Not appropriate for new developments ■ Cost of migration constrains replacement	■ Maintenance revenue focus
Obsolete	■ Rarely used	■ Used/resale market only

Source: Gartner (July 2020)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Cool Vendors in Privacy, 2020

Cool Vendors in Privacy Preservation in Analytics

Practical Privacy — Successfully Transition to Privacy-Preserving Marketing and Adtech

Practical Privacy — Four Fundamental Use Cases for International Data Transfers

Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria

Market Guide for Subject Rights Request Automation

Predicts 2020: Embrace Privacy and Overcome Ambiguity to Drive Digital Transformation

5 Areas Where AI Will Turbocharge Privacy Readiness

Privacy in a Pandemic: 5 Keys to Navigate the Disruption and Set Up for the Future

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp