The State of Privacy and Personal Data Protection, 2020-2022

Published 26 August 2020 - ID G00726093 - 27 min read

By Analysts Nader Henein, Bart Willemsen, Bernard Woo

Initiatives: Security and Risk Management Leaders; Privacy Program Management; Technology, Information and Resilience Risk

As the world adjusts to a "new normal" brought on by the COVID-19 pandemic, security and risk management leaders must adapt their privacy programs for better scale and performance as well as tighter budgets, all without exposing the business to loss through fines or reputational damages.

Overview

Key Challenges

- The pace of proposal for and adoption of modern privacy regulations accelerated through 2020, surpassing the record-breaking cadence in 2019. This has raised the stakes for organizations looking to standardize a global policy when handling personal data.
- Regulators have evolved to adapt with the notable increase in data subject complaints. They have shifted toward greater investigatory detail and more proactive actions signaling that expectations regarding privacy compliance have not normalized and continue to mount.
- Technology-driven capabilities supporting the facets of a progressive privacy program have developed substantially over the past 18 months, yet adoption lags, exposing organizations to expensive manual processes, fines and potential litigation.
- In the shadow of the global pandemic and the associated economic downturn, organizations are focused on cost optimization, this often leads to impulsive decisions to deprioritize compliance with all nonrevenue programs.

Recommendations

To treat technology, information and resilience risk, security and risk management leaders should:

- Incorporate the demands of a rapidly evolving privacy landscape into the organization's data strategy by developing a common baseline driven by applicable regulatory guidelines and privacy frameworks outlined in this research.

- Adopt key capabilities that support increasing volume, variety and velocity of personal data by putting in place a three-stage technology-enabled privacy program.
- Accept, adapt and evolve with the new business challenges to privacy by leading with a cost-optimized set of privacy capabilities.

Strategic Planning Assumption(s)

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

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

By 2023, companies that earn and maintain digital trust with customers will see 30% more digital commerce profits than their competitors.

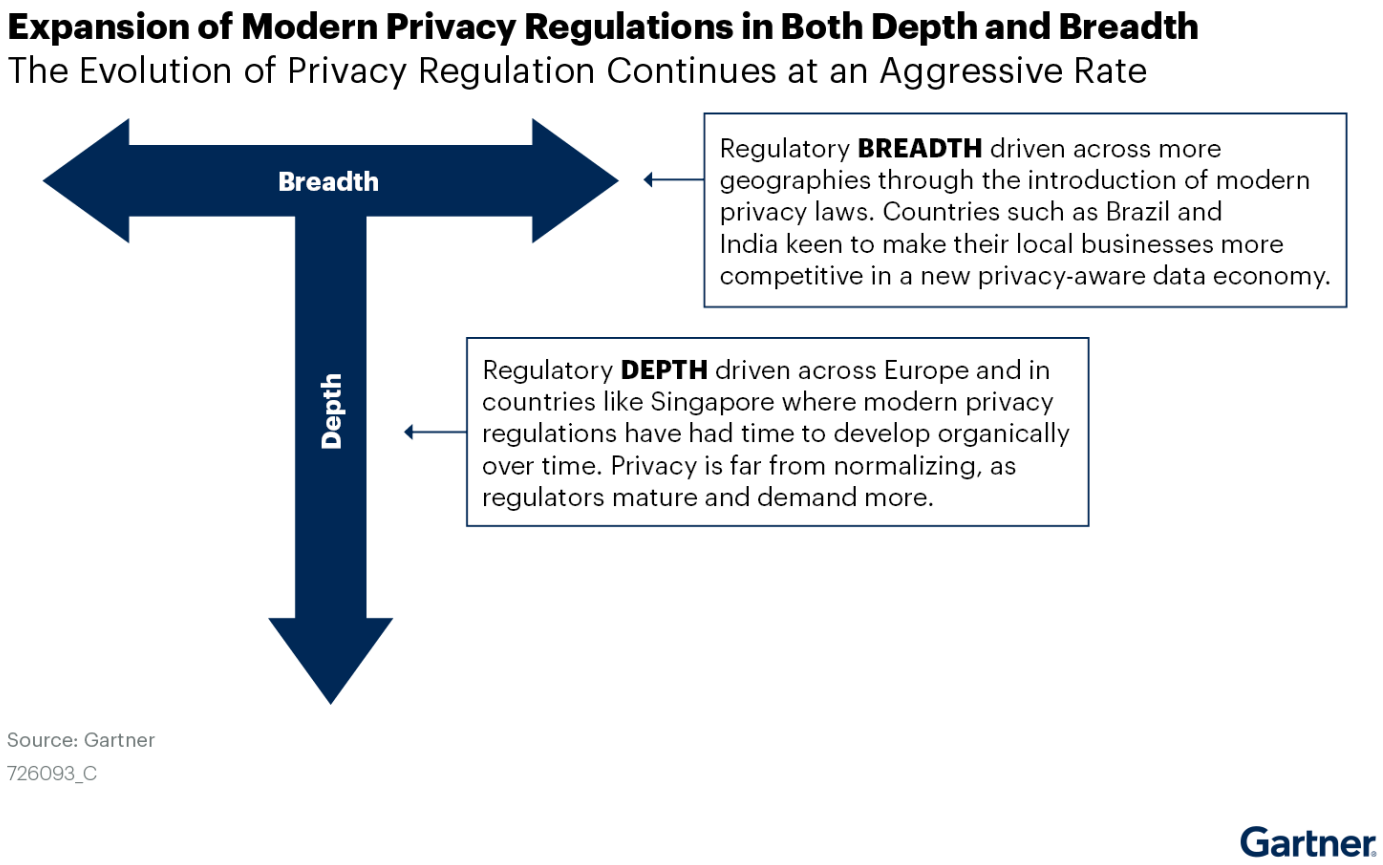
By 2024, more than 80% of organizations worldwide will face modern privacy and data protection requirements.

Introduction

"The state of privacy" is published in 18-month intervals to provide a two-year strategic outlook as well as the operational capabilities organizations will need to deliver and exceed growing regulatory and societal demands.

Privacy regulations across the globe have continued to develop aggressively two years on from the introduction of the General Data Protection Regulation (GDPR). In countries where modern privacy laws were established, regulators continue to drive depth increasing their expectations and proactive enforcement into areas that had previously been addressed only pursuant to a substantial volume of complaints. In contrast, breadth has been driven by the introduction of new legislation in countries that had not modernized their privacy regulation in decades and wish to join a new data economy (see Figure 1).

Figure 1. Expansion of Modern Privacy Regulations in Both Depth and Breadth



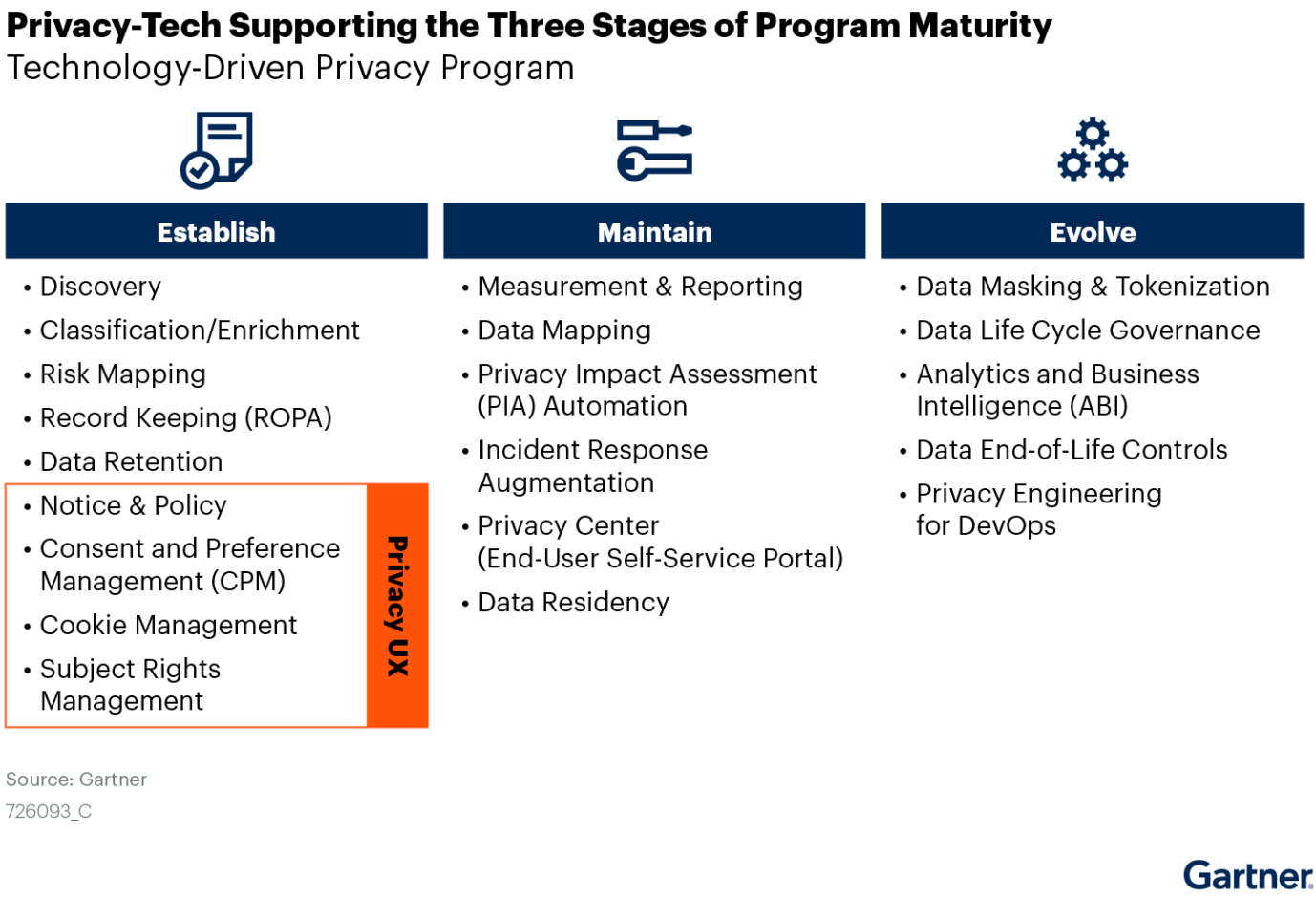
In almost all cases, new privacy laws (passed or proposed) have been heavily influenced by the GDPR, introducing concepts such as subject rights, explicit consent and timely breach disclosure. Regulatory changes are likely to continue over the coming two to three years, establishing the fundamental basis for privacy at the legislative level.

Consumer awareness and demand for privacy has also developed, often through confrontation with widespread use of new technology such as facial recognition in public places. [1]

Much like every facet of life, the global pandemic has pushed privacy concerns to the forefront, forcing governments to rethink their contact tracing initiatives and forcing businesses to adapt their employee monitoring to a work-from-home model.

Security and risk management (SRM) leaders should pay close attention, especially as it relates to the developments in the technology-enabled privacy landscape outlined in Figure 2. With cost optimization being a main focus in the boardroom, these practices will be the difference between exceeding expectations and insolvency.

Figure 2. Privacytech Supporting the Three Stages of Program Maturity



Analysis

Incorporate the Demands of a Rapidly Evolving Privacy Landscape Into the Organization's Data Strategy Program

Whether your organization works locally or operates globally, privacy regulations impact your decisions when processing personal data, which has become omnipresent in all facets of business.

The following regional breakdown provides both a roundup of recent key updates as well as clear recommendations for the coming year.

North America

Canada has taken the first steps toward reforming its federal private sector legislation, Personal Information Protection and Electronic Documents Act (PIPEDA). Proposals have been tabled and one area expected to receive focus is the expansion and alignment of individual rights in the direction of the GDPR. At the provincial level, Ontario amended its health sector law, the Personal Health Information Protection Act (PHIPA) to double the maximum financial penalties for noncompliance (up to CDN$1 million). In parallel, Quebec has tabled Bill 64 to overhaul its privacy regulatory framework (in both public and private sectors). Proposed changes are modeled after the GDPR and include a mandatory

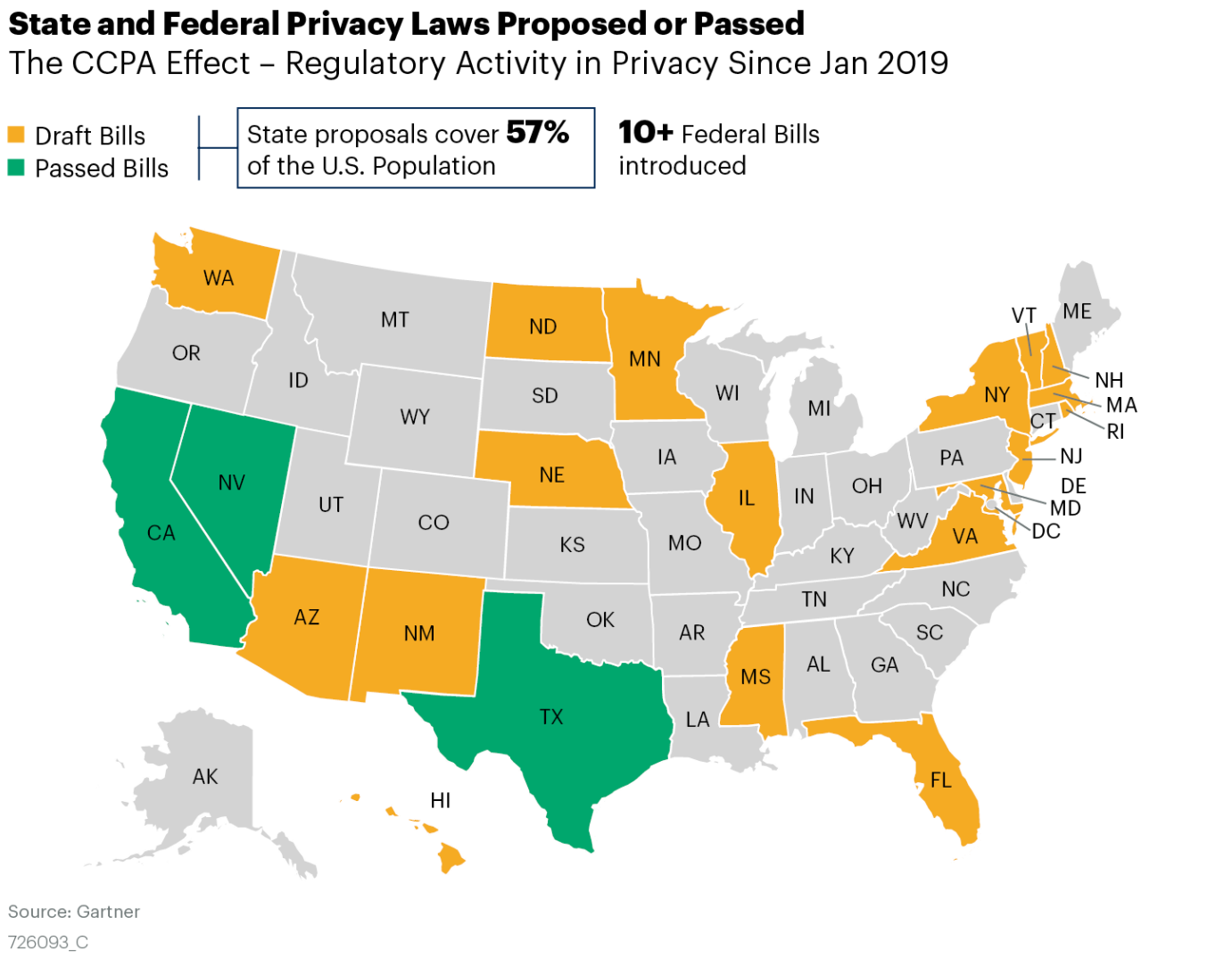
requirement for a data protection officer as well as a significant increase in sanctions for noncompliance (greater than CDN$25 million or 4% of worldwide turnover).

Further to the south, the ignition point for the modernization of U.S. privacy regulation has been the California Consumer Privacy Act (CCPA). The CCPA was passed almost unopposed], [2] came into effect [3] and subsequently came into force as of 1 July 2020. [4] Furthermore, the CCPA seems to be the first step in California's privacy journey as the California Privacy Rights Act (CPRA), commonly referred to as CCPA 2.0 emerged with 88% support among the voting public. [5]

The CPRA introduces further consumer rights, transparency requirements and the establishment of an agency (the California Privacy Protection Agency) to oversee enforcement.

As shown in Figure 3, at the time of publication, more than 20 states have followed suit, introducing draft laws, some of which exceed the CCPA in scope. Cumulatively, they impact more than 57% of the population in the U.S.

Figure 3. State and Federal Privacy Laws Proposed or Passed



Gartner

The federal push continues, with more than 10 bills put forward. The most recent is notable as it focuses on providing the American public with more transparency and control over their personal health, geolocation, and proximity data as it relates to the fight against COVID-19. [6]

A common approach we see with organizations is a focus on CCPA rights, not only for California residents but across the U.S. Whereas some organizations may be fixated on the fines, automation of subject rights requests (SRRs) toward a self-service model is by far the most sought-after capability.

Microsoft launched its global SRR self-service portal with the GDPR, and in the space of 18 months, it received 25 million requests, with 40% (almost 10 million) coming from the U.S. Had Microsoft simply provided a form and processed these requests manually, at the unrealistically low cost of $100 per request, it would have cost $1 billion in the U.S. alone.

SRM leaders tasked with preparation for a turbulent U.S. privacy landscape should focus on developing the organization's privacy UX capabilities, comprising privacy notice, consent and preference management and subject rights management (see the Adopt Key Capabilities That Support Increasing Volume, Variety and Velocity of Personal Information section) and standardizing against a CCPA inspired baseline. [7]

Europe

Two years into the GDPR and some of Europe's largest privacy regulators have signaled that they have adapted to the volume of complaints. This is an important milestone as it marks a notable shift from reactive, complaint-driven enforcement to proactive investigations and special projects orchestrated by the European Data Protection Board (EDPB).

As organizations look to normalize their privacy programs, this is not the time to slow down the development of the privacy program. Even with the global pandemic, regulators have signaled that they intend to be " pragmatic," but that there will be no easement of regulatory requirements, especially in the handling of employee/citizen health data relating to COVID-19 mitigation strategies.

SRM leaders should continue developing their privacy capabilities from the establish phase toward the *evolve* phase (see Figure 1), ensuring they match maturing regulatory expectations and achieve much needed cost optimization.

Special note regarding Brexit: as Brexit draws near (January 2021), it is becoming evident that organizations transferring data from Europe to the United Kingdom will have to make provisions to accommodate for cross-border transfers. Even though the Information Commissioner's Office (ICO; the U.K. privacy regulator) has indicated that it will pursue an adequacy ruling, a recent open letter from the EDPB [8] has shed serious doubts on the U.K.'s qualification given the government's signing of the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act. SRM leaders are advised to put in place mechanisms for the transfer of personal data from Europe to the U.K. as soon as possible, without having to rely on an expedited adequacy process.

Asia/Pacific

Australia introduced the Consumer Data Right (CDR) in July 2020. The CDR provides individuals with additional control over the processing of their data and will be rolled out on a sector-by-sector basis, starting with financial services.

After much anticipation and heated debate, the Civil Code was passed by the National People's Congress of **China** on 28 May 2020 and will be enacted on 1 January 2021. It is an extensive piece of legislation that will replace much of the existing civil laws. Of note is an entire section dedicated to the "Right of Privacy and Personal Information Protection," extending earlier legislation passed in 2017 as part of the Cybersecurity Law.

For organizations operating in the People's Republic of China (PRC), this will increase the cost associated with privacy violations, the increase will come in the form of civil liability in addition to criminal and administrative penalties stipulated under existing laws.

Of equal note is the updated Multi-Level Protection Scheme (MLPS) (v.2.0) that went into force 1 December 2019. MLPS 2.0 imposes heightened regulatory requirements around data protection and additional enforcement methods.

India's journey to modernize its privacy legislation continues. The Personal Data Protection Bill (PDPB), 2019 was introduced in Lok Sabha (parliament of India) on 11 December 2019. Expected to pass in late 2020 or early 2021 (due in part to delays related to COVID-19), the bill is an updated copy of the 2018 version, and has gone some way in addressing data residency restrictions that were a major sticking point.

New Zealand's parliament passed the Privacy Bill (June 2020), which repeals the 27-year old Privacy Act and sets the nation state on solid footing for personal data handling in line with the GDPR. The new law is expected to go into effect on 1 December 2020. Items amended include mandatory breach reporting and placing the onus on data controllers to ensure an adequate level of protection of personal data regardless of data residency.

Singapore's Personal Data Protection Commission (PDPC) has been ramping up enforcement and advisory practices indicating that it may be working toward EU adequacy, following in the footsteps of Japan (effective) and South Korea (upcoming).

South Korea passed legislative amendments to its data protection framework early 2020 to aid its efforts to gain adequacy standing with the EU. Changes introduced include the consolidation of enforcement duties under one body (Personal Information Protection Commission [PIPC]) and the concepts of pseudonymized information and purpose limitation (similar to the GDPR). The amendments had been targeted to go into effect during the fall but maybe delayed.

Thailand's Personal Data Protection Act (PDPA), which emulates much of the GDPR was set to go into effect in May of 2020, but has since been postponed for one year. The main reasons cited were related to relieving the regulatory burden as businesses and government agencies were focused on dealing with the effects of a global pandemic.

Asia/Pacific is on an irreversible trajectory for privacy modernization, moving to mature further since the revision of the APEC Framework. For international data transfers, a government-backed certification system named the Cross Border Privacy Rules (CBPR) was developed and endorsed by the 21 member states and recognized in trade agreements with Mexico and Canada. These developments across the privacy landscape in Asia/Pacific drive SRM leaders with existing or upcoming operations in the region to standardize against a GDPR-aligned baseline with provisions for data residency where required.

Latin America

The most discussed development is found in **Brazil.** Responsible for more than one-quarter of Latin America's GDP, Brazil has followed the European model quite closely with the Lei Geral de Proteção de Dados (LGPD). At the time of writing, the effective date of the LGPD remains uncertain, with conflicting news covering a gamut of options ranging from partial applicability to a one-year delay.

Brazil is not the only country in Latin America that follows EU-inspired trends. To date, **Uruguay** and **Argentina** are recognized by the European Commission as offering adequate data protection [9]; but both nations are due for their first reassessment post-GDPR. This has prompted a revision of national legislation to realign with the now effective, more holistic GDPR. Argentina began drafting updates in 2016 and has already seen a presidential proposal to replace its existing legislation to align better with Brazil and the EU.

In addition, **Mexico** became the 53rd country to undersign Convention 108, [10] and will make changes to their national data protection legislation in line with the treaty. Convention 108 is an international treaty designed to provide a certain uniformity to how individuals' personal data is protected, enabling privacy rights and preventing data misuse.

Chile has a data protection law [11] in place and is also looking to update with a combined bill, more in the spirit of GDPR, including purposeful processing and proportionality. Chile aims to align with the Organisation for Economic Co-operation and Development (OECD) membership requirements and position itself as a "safe harbour" jurisdiction for international transfers, establishing a formal data protection authority and acknowledging various privacy rights.

Similar developments are underway in **Peru** through updates of the existing privacy laws (Bill 1828 of 2011 [see Note 1]) and in **Colombia**, where revisions of Law 1581 are suggested through Bill 91 of 2016 and are currently under debate. **Panama's** recent data protection law [12] is light on detail comparatively.

Knowing there are severe reputational risks added to the financial sanctions for noncompliance, SRM leaders should establish a foundational privacy management program aligned to the GDPR framework (see "Toolkit: Setting Up a Privacy Program").

Best practices for SRM leaders are further outlined in "What You Need to Know About Privacy in LATAM."

Africa and the Middle East

Over the past 12 months, the Middle East and North Africa have seen a fair bit of movement. Privacy regulations have come into effect in **Bahrain** (the Personal Data Protection Law, effective 1 August 2019), the **United Arab Emirates** (modernized DIFC Data Protection Law, effective 1 July 2020) and **Egypt** (the Personal Data Protection Law, effective 15 October 2020), all heavily influenced by the GDPR. Further regulation is expected in Saudi Arabia and potentially sooner in Oman.

Africa has also seen its share of change, with its two largest economies putting privacy on the books. In **South Africa,** the Protection of Personal Information (POPI) Act, delayed due to COVID-19 but taking effect 1 July 2021. To the north, in **Nigeria,** the Data Protection Regulation, effective 25 October 2019 is

being tested in a recent lawsuit filed by the Laws and Rights Awareness Initiative, an NGO against Chinese social media giant TikTok.

The Way Forward

As predicted in "The State of Privacy and Personal Data Protection, 2019-2020," with more countries introducing modern privacy laws in the same vein as the GDPR, we have crossed a threshold where the European baseline for handling personal information is now the de facto global standard.

Through globalization, the EDPB has motivated lawmakers to raise their countries' data-handling standards. As they introduce privacy laws, working toward parity with the GDPR, they move one step closer to achieving adequacy with the EU, where their local businesses can benefit from a larger market with their new "trusted" status. There is no better example of the added complexity businesses face in the absence of adequacy than the turmoil caused following the invalidation of Privacy Shield, [13] the mechanism through which thousands of organizations transferred personal data from Europe to the U.S., in July of 2020.

Security and risk management leaders should enforce a comprehensive privacy standard in line with the GDPR. This will allow their businesses to differentiate themselves in an increasingly competitive market and grow unhindered.

Adopt Key Capabilities That Support Increasing Volume, Variety and Velocity of Personal Information

We break down the technology-enabled privacy program into three stages of traditional adoption — establish, maintain and evolve — as outlined in Figure 2. This is not to say that an organization in the early stages of its privacy program cannot choose to use capabilities from the Evolve stage. Instead, the need varies based on the business drivers and the associated privacy risk.

Establish

This stage outlines foundational capabilities of a privacy management program. These are considered necessary tools for any customer-facing organization that processes personal information:

- **Discovery.** These include a variety of tools providing the capacity to locate personal data in structured, unstructured and semistructured silos indexed by individual user identifiers. This capability is necessary to take stock and maintain awareness as to the location of personal data within the organization's applications, databases and repositories. Note that these capabilities should be effective in both cloud-based and on-premises processing activities.

Associated Research: "Practical Privacy — Discovery Automation of Privacy Risk" covers discovery as well as classification/enrichment and risk mapping.

- **Classification/Enrichment.** This involves attaching the appropriate metadata (in the form of tags or labels) to existing and new personal information. The process is necessary to enable operational

functions such as privacy-risk-based scoring and granular data retention policies, as well as fulfillment of SRRs. Metadata enrichment enables dynamic controls, providing value well beyond the privacy program. A rich understanding of data allows for governance agility, giving organizations the capacity to absorb the impact, react and adapt to new regulations with minimal disruption to operations.

- **Risk Mapping.** This involves risk assessment and tracking across different repositories and applications where personal data is processed. Tools are needed to review personal datasets, factoring in classification and domain-specific knowledge. The end result includes privacy risk registers for data repositories, applications and vendors where personal data is associated with risk scores. This then drives risk-based prioritization and subsequent mitigation.

- **Record Keeping.** These functions support documenting records of processing activities (ROPAs) when personal information is handled. This is an explicit requirement under laws like the GDPR and the LGPD, but it is an implicit necessity to demonstrate proper handling of personal data. A ROPA demonstrates who has accessed the data and for what purpose, as well as which parties it was shared with. These logs are needed to allow for auditing and validation of purposeful processing.

- **Data Retention.** In the Establish stage, data retention (previously data minimization) focuses on deletion of large batches of data that are no longer in use and that do not have any regulatory retention requirement. At higher levels of organizational maturity, this shifts to the more targeted "end of life controls" to reduce the privacy risk and maintain utility.

Associated Research: "Practical Privacy — Managing Data Retention and Backups"

- **Privacy UX.** Privacy user experience, or privacy UX, encompasses the full range of functions centered around the handling of an individual's personal information when interacting with an organization. This experience includes privacy notices, data acquisition (through forms, cookies or otherwise), preference and consent management, and subject rights management:

Associated Research: "Practical Privacy — A Definitive Guide to Privacy UX"

- **Notice and Policy.** Internal privacy notices and external privacy policies are two sides of the same coin. One is the commitment to users as to how the organization will handle their personal information, and the other provides detailed guidance to employees and contractors to deliver on that promise. Notices and policies must be regularly reviewed and updated to align with regulatory requirements and consumer expectation; reviews should be conducted yearly. Tools exist that can track these notices and policies across multiple external sites and internal portals to ensure they are kept up to date and regularly reviewed. Tracking of these policies over time is also critical to review the information provided to users against which they gave their consent.

Associated Research: "Toolkit: Privacy Policy"

- **Universal Consent and Preference Management (UCPM; Inclusive of Cookie Management).** The consent and preference management market comprises an ecosystem of vendor services that consolidate end-user choices regarding how their personal data should be handled. This is then synchronized across a variety of legacy, active and incoming repositories, both on-premises and in the cloud. The ultimate intent is to extend visibility and control to users, allowing them self-determination over how much of their data to expose, to whom and for what purpose, with the option of changing these preferences at will.

Associated Research: "Market Guide for Consent and Preference Management"

- **Subject Rights Management**: SRRs are a family of requirements under law (such as the EU's GDPR, Brazil's LGPD or the CCPA), where organizations owe a structured response to individuals, explaining how they handle personal data and extending certain controls as to its use. Execution of SRRs requires an established privacy management program with clear workflows for involved departments, extending toward automation and self-service.

Associated Research: "Market Guide for Subject Rights Request Automation"

Vendors Versus Capabilities: Some privacy vendors provide point solutions that specialize in a singular capability (such as consent and preference management). Others will combine a few capabilities to provide an operational function (such as CCPA compliance through a combination of discovery, subject rights management and basic consent). There is also a growing class of mature, turnkey vendors, often referred to as privacy management solutions, that offer most if not all the capabilities across the Establish stage and some of those in Maintain stage on one comprehensive platform.

Maintain

This stage allows organizations to maintain their privacy management program over time. Capabilities focus on ongoing administration, resource management and scalability of recurring tasks. Many of the capabilities in this stage are driven by constraints faced in the earlier part of an organization's privacy management program:

- **Measurement and Reporting.** These capabilities track the efficiency of a privacy program through quantitative metrics. At the start, this is done by measuring metrics such as SRR fulfillment (time, cost and scale) or privacy impact assessment (PIA) completion. At higher levels of maturity, measurement shifts to quantify the extent of anonymity to offset privacy risk and tracking reidentifiability.

Associated Research: "IT Score for Privacy"

- **Data Mapping.** Often implemented through a series of application connectors and network probes, data mapping allows organizations to create a snapshot of personal data flows for on-premises as well as cloud systems.

- **PIA Automation.** PIAs are one of the cornerstones of the privacy management program, although many organizations will start by conducting the process manually through a series of spreadsheets and questionnaires. This process will become difficult to administer. It also traps the skills needed to conduct PIAs with a few people rather than making part of an organization's data-handling fabric. PIA automation tools allow for API-driven triggers to initiate the assessment process, tracking it through a predefined workflow all the way until a case is closed or flagged for remediation.

Associated Research: "Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria"

- **Incident Response Augmentation.** Most organizations will have an incident management process. Privacy-related incidents (inclusive of breaches) demand augmenting existing processes to swiftly assess whether an incident requires disclosure. Solutions in the market will allow for incident handling to branch in the case of a privacy-related occurrence so that the data protection team can be engaged, and appropriate steps can be taken.

- **Privacy Center.** Also referred to as "self-service portals," these capabilities allow users to view their data and how it is used, and to administer their consent choices. Well-developed preference centers elevate an organization into a higher level of privacy management maturity, placing control back into the individual's hands, allowing for a frictionless subject rights fulfillment experience.

- **Data Residency.** Data residency is an emerging requirement in multiple privacy laws. It requires restricting data storage and/or processing to a defined geography. Tools in this space either scan data in transit or leverage tags created in the classification/enrichment process to limit transfer altogether or mask data prior to the transfer.

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

Evolve

The Evolve stage includes specialist tools that focus on reducing privacy risk with little or no impact on the organization's utility:

- **Data Masking and Tokenization.** Deleting personal data is not the only way to manage risk. The target is not to merely purge, but also to reduce the risk to an acceptable level in line with the organization's risk appetite. Purposeful processing requirements primarily dictate that personal data is not processed in its raw state; rather, it is treated (masked through techniques such as anonymization or pseudonymization) for the purpose of processing and with the explicit intent of reducing risk to individual privacy. Tools in this category should also provide the capability to test the efficacy of the treated datasets regularly so as to confirm that the effort involved in reidentification is balanced with the risk that the data represents.

Associated Research: "Market Guide for Data Masking"

- **Data Life Cycle Governance.** These capabilities allow administrators to automate tracking and introduce rules for a piece of data from birth to death as it flows through the organization: how it is used, for what purpose, and by whom.

- **Analytics and Business Intelligence (ABI).** Analytics represents one of the more difficult challenges to address in the privacy program. Solutions in this space are complex and often rely on equally complex technologies, such as differential privacy or secure multiparty computation (SMPC). This allows organizations to mine large data lakes for insight while safeguarding individual privacy rights and generating shared insight from multiple sources without sharing the raw data.

Associated Research: "Achieving Data Security Through Privacy-Enhanced Computation Techniques"

- **Data End-of-Life Controls.** As organizations understand their data better, meticulous and automated privacy risk retirement becomes commonplace. Organizations can choose from a list of risk reduction methodologies to treat personal information at end of life with a balanced, risk-based approach in both production and offline storage/backup environments.

- **Privacy Engineering for DevOps.** Privacy engineering takes the principles of privacy by design (PbD) and folds them into the DevOps life cycle to programmatically enforce foundational requirements, such as purpose limitation and ensuring a lawful basis for processing.

Associated Research: "Build for Privacy"

Implement Cost Optimization in the Adoption of Privacy Capabilities

As security and risk management leaders realign their priorities against a shared business reality because of the global pandemic, cost optimization is placed at the top of the list. Luckily, "privacytech" has never been an expensive line item, especially when compared with other technology investments. Furthermore, privacy, independent of being a regulatory requirement, brings quantifiable business benefit especially for B2C and B2B2C organizations. So, in an ROI calculation, privacy investment resides toward the top of the list.

It's worth noting that the challenge of setting up and maintaining a privacy program is very much proportional to the amount of data handled, the number of users and the complexity of the environment. As such, the undertaking is, in most cases, proportionate to the size of the organization.

Before a single penny is spent, any organization starting its privacy program should assess where it stands. The "IT Score for Privacy" is an excellent measure of just that. It allows organizations to evaluate their capabilities, determine where improvements will add value and develop a roadmap to enhance privacy risk management. The assessment also allows organizations to benchmark themselves against the mean of businesses in their field and can be rerun at regular intervals to track improvements and provide ongoing feedback to leadership.

For Startups and Small Businesses

Running a privacy program manually through a combination of workflow solutions, project management software and staff-hours can be achieved, but it's quite taxing and prone to error. Consider employing a turnkey privacy platform for a less onerous and more consistent approach.

Cost optimization: Some solutions offer freemium or consumption-based licensing models. These substantially lower the bar toward adoption and allow the business to keep costs under control.

Team size: One to two shared resources with potential for outsourcing of the privacy function altogether.

For Midsize Organizations

It's always recommended to start manually and get a better feel for the data and the complexity of the task at hand. However, we consistently see businesses fast realizing that automation is a necessity across areas such as discovery, consent and subject rights management. Consider a privacy management platform with optional point solutions where complexity or specialist capabilities are required.

Cost optimization: Look toward capabilities within existing enterprise solutions already in use within the enterprise. These could include discovery in master data management (MDM) or subject rights management within CRM or IT service management platforms, as well as governance capabilities built into email and productivity suites.

Team size: Two to four full-time equivalents (FTEs) with privacy champions (optional) in departments where large-scale or high-risk personal data is processed.

For Large Enterprise

Larger organizations often need specialist capabilities, which leads to substantial fragmentation. In organizations potentially spanning countries and verticals, and faced with a complex web of regulatory requirements, we regularly see multiple turnkey platforms and multiple point solutions in different business units across different geographies.

Cost optimization: Establishing one set of rules and one consolidated technology approach (with multiple vendors) capable of adapting to exceptions when needed has and will save large enterprises hundreds of thousands of dollars in redundant spend. The main linchpin is centralized management of the operational privacy function.

Team size: Four to eight FTEs with privacy champions (required) in departments where large-scale or high-risk personal data is processed.

Notes:

- Recommended team sizes do not include mandated roles, such as data protection officers, required by law in Europe.

- The definition of small, midsize and large is not tied to a set number of employees as different size organizations in different geographies are classified differently.

Evidence

[1] "UK's Facial Recognition Technology 'Breaches Privacy Rights'," The Guardian. (Free registration required.)

[2] "AB-375 Privacy: Personal Information: Businesses," California Legislative Information.

[3] "California's Groundbreaking Privacy Law Takes Effect in January. What Does It Do?," The Guardian.

[4] "CCPA Enforcement To Begin On Wednesday July 1, 2020 — Steps to Get Ready," Forbes.

[5] "ICYMI: Summary of Key Findings From California Privacy Survey," Californians for Consumer Privacy.

[6] "Wicker, Thune, Moran, Blackburn Announce Plans to Introduce Data Privacy Bill," U.S. Senate Committee on Commerce, Science, & Transportation.

[7] "Microsoft Will Honor California's New Privacy Rights Throughout the United States," Microsoft Blog.

[8] Letter from the EDPB regarding the agreement between the U.K. and the U.S., EDPB.

[9] "Adequacy Decisions," European Commission.

[10] "Convention 108 and Protocols," Council of Europe.

[11] "Chile: Data Protection 2019," International Comparative Legal Guides.

[12] "Finally Panama Has a Data Privacy Law," Lexology.

[13] " Statement on the ECJ Judgment," European Data Protection Board.

Note 1. Privacy Legislation in Latin America

The various jurisdictions have both existing laws in place, as well as multiple draft bills circulating for review and revision. Not all countries in Latin America are part of this analysis; only the most inquired after regions are taken into account. The best practices described are selected for their fit with both existing laws and with parts of various draft bills that the author(s) had access to. Because parts of draft material are not publicly available, we will reference here only the links to existing laws in effect:

Argentina: Protección de los Datos Personales, Ley 25.326

Brazil: Lei Geral de Proteção de Dados Pessoais (LGPD), taking effect in 2020

Chile: Law 19628, and a bill to modify it

Colombia: Ley 1581 de 2012 Nivel Nacional (statutory law regulating the processing of personal data, as well as databases)

Mexico: Various components of law regulate the handling of personal data, starting with a federal law of 2011. Most important is the latest addition (until revision is completed as expected to realign further with modern privacy laws) of the law for the Protection of Personal Data in Possession of Obligated Subjects LGPDP-PSO

Peru: Ley de Protección de Datos Personales (LPDP)

Uruguay: Ley N° 18331

Recommended by the Authors

Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria

Hype Cycle for Privacy, 2020