FUTURE OF PRIVACY FORUM

MARCH 2022

PRIVACY METRICS REPORT

AUTHORED BY

Omer Tene

Senior Fellow, Future of Privacy Forum

Mary Culnan

Board Vice President & Senior Fellow,
Future of Privacy Forum

ACKNOWLEDGMENTS

This paper benefited from contributions and editing support from the FPF Privacy Metrics Working Group and Judy Gawczynski, Membership Director, Future of Privacy Forum.

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

Table of Contents

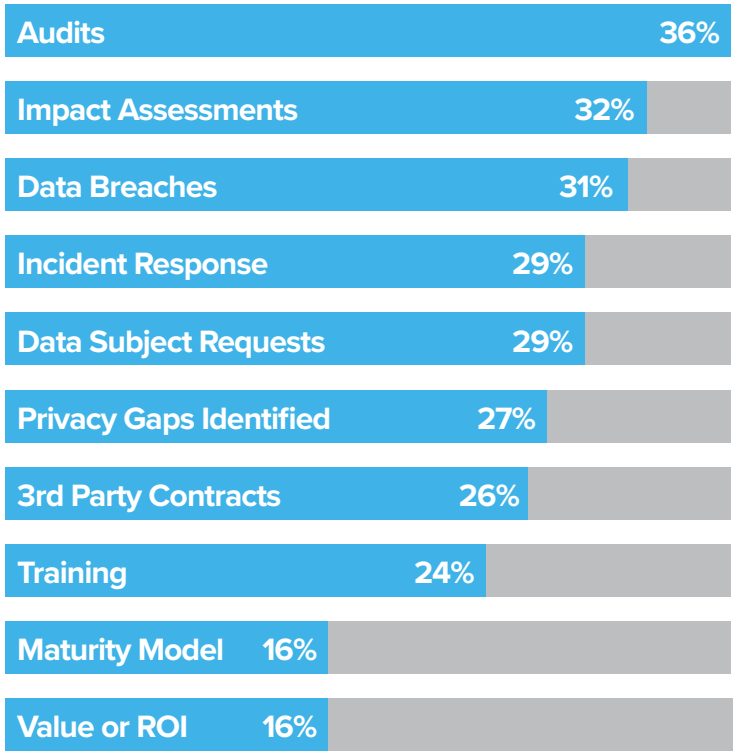
Introduction

The EU's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), as well as the constant drumbeat of major data breaches have ushered in a new era in privacy and data protection accountability and awareness, elevating privacy beyond the office of the privacy leader to the attention of boards of directors, audit and risk committees, CEOs, CIOs, CROs, CISOs and more (internally), and to the view of customers, legislators, regulators, advocates and the media (externally). Organizations have expanded their privacy and data protection programs to cultivate customer trust and loyalty; to enable secure cross border data transfers; and to comply with evolving and dynamic privacy laws and regulations. Over the past few years, privacy governance has emerged as a core business value central to customers' and employees' trust, as well as for core corporate values such as transparency and accountability. A wave of media maelstroms, diplomatic rows, and litigation crises — as well as competitive developments in markets, companies, and platforms — have shown that inadequate privacy is bad for business. With a new wave of regulation on the horizon, including global privacy legislation as well as rules for artificial intelligence, digital services, and platforms and non-personal data, the remit of privacy officers is set to grow even more.

Business leaders have traditionally advocated for management by measurement. Edwards Deming wrote, "What gets measured gets done." Dr. H. James Harrington once said, "If you can't measure something, you can't understand it. If you can't understand it, you can't control it." Effective measurement helps managers improve efficiency, streamline processes, prioritize efforts, and manage risk. Indeed, some say that measurement is management.

Privacy leaders collect data and use metrics to measure, assess, and improve the performance of their privacy programs. Beyond demonstrating compliance, privacy metrics have emerged as key to measure and improve privacy program performance and maturity in terms of customer trust, risk mitigation, and business enablement. Privacy leaders use metrics to benchmark the maturity of their organization's privacy program against its strategy and goals and demonstrate how privacy contributes to its strategy and bottom line. They use metrics internally to secure budgets and staffing, to measure performance and to diagnose program status and needs, as well as externally to demonstrate accountability and enhance trust. They use metrics to measure, for example, how sound privacy practices reduce sales delays, mitigate

Privacy Metrics Reported to the Board of Directors



Source: Cisco 2021 Data Privacy Benchmarking Study

impacts from data breaches, enable innovation, achieve operational efficiency, build trust with customers, and make the organization more attractive for customers and shareholders. They increasingly report metrics to boards of directors, an indication of the growing sophistication and maturity of privacy programs and the coming of age of privacy as a core business function, key for trust, brand, reputation, and risk mitigation.

While different sized businesses vary in their governance focus, according to Cisco's 2021 Data Privacy Benchmark Study, 93% of organizations are now reporting at least one privacy metric to the board of directors, with 14% reporting five or more privacy metrics. Among the most reported metrics are Privacy Program Audit findings (36%), Privacy Impact Assessments (32%), and Data Breaches (31%).

Modern privacy laws, such as the California Consumer Privacy Act (CCPA), create regulatory mandates specifying privacy metrics that organizations must report. By becoming sophisticated curators of privacy metrics, organizations can not only satisfy legal requirements but also contribute to a market driven standardization of privacy metrics as opposed to their determination by legislative fiat.

This report, which is based on discussions held at the FPF Privacy Metrics Working Group, reviews the types of privacy metrics that organizations deploy to assess legal compliance, proactively manage risk, enhance customer trust and enable business processes. It sets forth various purposes and audiences for privacy metrics; common metrics used in organizations; the use of metrics for risk management and benchmarking; and tools used to collect data to compile metrics. It provides examples and tangible suggestions for organizations on how to resolve real world challenges that often arise when collecting, curating and presenting privacy metrics. While suggesting various metrics that would be appropriate for different audiences ranging from the Chief Privacy Officer to the Board of Directors, the report does not advocate a one size fits all prescription. Instead, organizations should adopt metrics that are appropriate for the context, goals, resources, and maturity of their privacy programs. For example, a small organization will likely adopt a different set of metrics than a large multinational corporation.

Privacy Metrics: A Definition

Privacy metrics are both quantitative and qualitative assessments that privacy leaders use to measure, manage, track, benchmark, report on, and improve their privacy program and its components and to establish transparency and trust.[1] Specifically, privacy teams may adopt the SMART Framework (Specific, Measurable, Actionable, Relevant and Time Bound) to create SMART privacy metrics to assess their capabilities and fulfillment of objectives, demonstrating the relevancy of each metric while ensuring the completion of tasks within specified time frames.

Purposes and Goals

Privacy programs use metrics for a variety of purposes and goals: compliance, operational, business imperatives, and external uses. To be effective, metrics should be assessed against clearly defined privacy program objectives and goals.

Compliance uses include measuring and tracking key metrics that demonstrate compliance with various laws and regulations. This includes tracking progress to achieve compliance with applicable requirements, as well as helping to ensure sustainable compliance over time.

Operational uses include measuring, documenting, and improving the performance of the privacy program; managing enterprise privacy risks; and making progress toward meeting the privacy program's objectives and goals. In the first instance, this means ensuring the organization complies with its corporate policies, standards, procedures, and applicable privacy and data protection laws and regulations. Examples include metrics for incident reporting and measures related to data sharing with business partners and service providers, including cross border data transfers.

1 Not just privacy leaders but also other staff at all levels of the organization collect, use and present privacy metrics. In this report we use "privacy leaders" as shorthand to address various stakeholders in charge of privacy metrics.

This also involves pursuing internal goals and objectives, such as privacy training and awareness or service-level agreements (SLAs) for privacy enterprise risk assessments. Privacy leaders use metrics to help align the priorities of the organization, identify high risk areas, and allocate funding or headcount. They identify program targets in annual planning and use metrics to demonstrate progress toward achievement of these goals. They use metrics to identify operational anomalies and serve as early warning signals that warrant further investigation. They deploy metrics to help drive compliance in the business, highlighting gaps and outstanding issues and tracking the business' progress in addressing them.

Privacy leaders also use metrics to assess or benchmark the operational maturity of their organization's privacy program compared to relevant industry standards, regulatory frameworks or competitor practices as well as to focus and drive program improvements. They address the mitigation of privacy related risks, including compliance and litigation, incidents, disruption of business, and brand impact. Privacy maturity models are means for a company to organize and simplify the complexity of the privacy environment and to measure the progress of its policies and operations against established benchmarks. For example, the AICPA/CICA privacy maturity model maps the ten privacy principles of the Generally Accepted Privacy Principles (GAPP) against five maturity levels (Ad hoc, Repeatable, Defined, Managed, and Optimized). For the access principle, for instance, the privacy maturity model assesses how an organization's policies address providing individuals with access to their personal information, including how the organization communicates with individuals about their access rights and how it authenticates their identity.

Business Imperative uses focus on customer engagement and business enablement. *Customer engagement* metrics measure an activity or behavior of interest to decision makers such as facilitating market access for products and services; assessing how privacy programs contribute to customer satisfaction; encouraging data sharing; and supporting user engagement and trust. This includes appropriate privacy oversight of authorized third party data processors (e.g., service providers, suppliers, vendors) who are engaged in data processing activities on behalf of a business; incorporation of privacy by design into products; personal data lifecycle management and technology development; conducting privacy and data protection impact assessments (PIAs and DPIAs) for applications that potentially pose privacy risks; responding to incidents; and processing data subject access or deletion requests (DSRs) or customer privacy inquiries.

Business enablement metrics track the ability of privacy programs to support strategic business priorities, controls and processes; adopt new technologies; and create privacy operational excellence.

External uses include enhancing brand reputation; differentiating from competitors through thought leadership, advocacy, transparency, and best practices; demonstrating privacy credentials to customers; and engaging with policymakers (including legislators, advocates, academics), standards bodies and regulators. Advanced programs use privacy metrics for public policy goals, including following legislative and regulatory initiatives and trends, and engaging with and proposing new regulations.

Audiences

Privacy program leaders use metrics to communicate with various stakeholders. A key task for privacy leaders involves fashioning metrics into a *narrative*, that is, telling a relevant story to different stakeholders, ranging from the C-Suite, board audit or risk committee and other business or functional departments to external stakeholders such as consumers, business customers, regulators, privacy advocates, and the media. As one member put it, "privacy metrics are less about numbers, more about stories." Privacy leaders consider which audiences receive what metric reports and how to best leverage the reports. Different metrics resonate differently depending on the audience. For example, members of the privacy team will view different reports than those presented to legal, compliance officers, or business leaders. Business leaders tend to live and manage by metrics and could be presented, for example, with narrowly tailored or comparative reports.

The following chart specifies various audiences for privacy metrics, including the nature of metrics often presented to each group and the purposes for reporting to it:

Stakeholders	Nature of Metric	Purpose of Reporting Metrics
Executives (CEO/ Board of Directors)	• High level description of risk and program maturity • Material Incidents	• Ensure buy in/support • Proper allocation of staff/resources to risks • Report on risk/impact on bottom line • Report on program maturity/status/progress
Senior Leadership (GC, CIO, CISO, CITO, CDO, CMO, CRO)	• In-depth review of risk • Impact of risk-based approaches • Incident numbers and trends • Program Implementation progress/ spend • High-level benchmarking results	• Ensure buy in/support and executive oversight • Risk acceptance/decisions • Triage priorities • Control effectiveness and maturity • Ensure support in gathering data
Privacy Team	• Periodic comprehensive risk assessment • Reviews of program status, incident numbers and trends, implementation of controls, vendor management metrics, transactional, operational, and performance metrics • Privacy, data protection and transfer impact assessments, and vendor questionnaires	• Issue spotting: control program effectiveness/ remediate problems or gaps/enhance maturity • Information/dashboards to drive or inform key stakeholder interactions • Getting team aligned on most important goals • Internal allocation of resources • Performance reviews
Business Units	• Project/Product risks and compliance • Accountability/Performance • Risk Assessments • Progress in implementing new requirements/addressing known issues	• Communicate with marketing, HR, products, engineering, and business partner teams to ensure issue spotting, compliance, privacy by design • Hold business units to account for managing their privacy risk
External	• Privacy Impact Assessments (PIAs), Data Protection Impact Assessments (DPIAs) • Regulators, self-regulatory bodies and/ or external auditors: accountability mapping, Record of Processing Activities (ROPAs), PIAs, DPIAs, TIAs, incident information • Media and advocates: compliance and business enablement	• Customers: transparency and trust, differentiate brand • Regulators: compliance, demonstrating accountability • Investors and shareholders: demonstrating compliance and program effectiveness • Advocates: communicating policies and accountability • Media: maintaining brand reputation
Internal Audit and Risk Management	• Per request	• Evidencing/monitoring compliance, risks, costs, and remediation
Employees	• Training and awareness • Risk assessments • Business enablement • Material program implementation updates	• Ease of engaging with privacy team • Training and awareness • For sales employees/relationship managers: ability to share privacy practices and protections with customers for differentiation • Increase eNPS (employee Net Promoter Score)

Common Metrics

While different organizations measure different activities and trends, there is a common core of privacy metrics that many organizations collect and report on. Most organizations measure daily privacy program activities: counting the number of individual complaints and requests; responding to incidents or breaches; offering privacy compliance and awareness training to team members and employees; conducting data mapping; undertaking privacy, data protection, and transfer impact assessments; negotiating and executing data processing agreements; and so forth. Of course, collecting accurate and comprehensive data is a key step toward assembling effective metrics. Sound metrics require good data inputs.

Organizations vary in the categories and specific metrics they collect and report. The chart below, while by no means comprehensive, is illustrative of some common metrics.

Common Metrics Chart

CATEGORY	ITEM	METRICS
Individual Rights	Data Subject Requests (DSRs), Deletion Requests and Processing Objections	• Received • Closed • In progress • Duration • % satisfied and % satisfied within required time • Requests by type, region, SLA times
	Privacy Incidents/Breaches	• # of incidents by type/severity/business unit/entity/region • # of impacted customers • % of incidents by type, closed with SLA commitments • % of incidents where root cause has been identified and corrective action taken • # and % of incidents notified to regulators and data subjects • # and % of incidents reported within X hours/days of determination • Mean Time to Discovery (measure of detective capability) • Mean Time to Resolve (measure of efficiency of processes)
	Privacy Complaints	Similar
	Privacy General Queries	Similar
	Consent	• Data “sale” and cookie opt outs • Consent for processing activity • Consent for data sharing • Opt in consent for email marketing

Common Metrics Chart

CATEGORY	ITEM	METRICS
Training and Awareness	Privacy Trainings Privacy Awareness and Education	• Offered • Employees trained • % of Targeted Employee Base Completed Training on Time • Attendees (in person) • % of employees passing privacy challenge • # of privacy certifications obtained • # of additional enablement materials created and viewed (e.g., awareness emails, news clippings, white papers, web pages, website visitors, internal playbooks, privacy champion BUs, privacy champions)
	Privacy FAQs Processes and guidelines established	• Employee engagement • Functions in the organization that privacy engages with and who are the most frequent customers
Commercial	Data Processing Agreements (DPAs) Security/data protection addenda	• Negotiated customer • Closed customer • Negotiated vendor • Closed vendor • Tracking materially altered terms from standardized language • Timeframes to closure
	Vendor reviews	• Vendor privacy reviews/risk assessments (# completed, # in process, # planned, # scores) • Vendor control assessments (# completed, # in process, # planned, findings) • PCI/DSS assessments and status for each vendor • Vendor privacy compliance issues (#, severity, status against target closure date, etc.)
	RFI/RFP	• Privacy compliance attestation requests completed • Timeframes to completion • # of standardized privacy RFI/RFP Q&A available
	M&As/Divestitures/TSA/Joint Ventures	• Negotiated/closed • Time to complete privacy due diligence • Number of remediation actions identified
	Supply Chain	• # Agreements for Data Sharing • % Agreements with privacy contractual language

Common Metrics Chart

CATEGORY	ITEM	METRICS
Accountability	Policies and procedures Notices (consumers, employees)	• # inventory • Whether current • Date last updated/reviewed
	Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs)	• # of identified high risk data processing activities requiring a DPIA (as a % of total processing activities recorded/as a % of initial screening/ gating assessments) • # of PIAs/DPIAs completed • Time vs SLA
	Transfer Impact Assessments (TIAs)	• # of transfer impact assessments (post Schrems II) • # of vendor questionnaires
	Data Mapping/Records of Processing Activities (ROPAs)	• # of applications data mapped • # of applications that require data mapping • % of required applications mapped/not mapped • # of completed ROPAs
	Projects/products advised on	• # of marketing activities advised on • # of HR activities advised on • # of new business/models/technology solutions advised on (e.g., cloud as a service) • # of cross-functional projects
	Regulatory	• # of regulator inquiries (type, opened, closed)
	Business Unit/Function	Per Business Unit: • Privacy Steward/Accountable person appointed? (Y/N) • Business Unit privacy operating model in place and documented? (Y/N) • # and % privacy compliant apps processing PI • Progress status (R/Y/G or % complete) for outstanding BAU or regulatory change implementation actions • # and status (on track, overdue) of compliance monitoring/audit actions

Common Metrics Chart		
CATEGORY	**ITEM**	**METRICS**
Privacy Stewards (hub & spoke)	Privacy projects in product teams	• # of Personal Information Management Systems (PIMS) remediated • # of DPIAs supported • # of Rules of Procedure (ROPs) supported • # of department personal data use reviews for data extraction • # of cross-functional privacy projects • # of DSRs supported • # of department specific data privacy trainings offered • # of data privacy FAQs and awareness communications created (department/role-specific)
Policy	Legislative work Investor Ratings and Environmental Social Governance (ESG)	• Bills monitored • New laws • Review status • Rating agency scores

While basic metrics measure *activities* (e.g., number of DSRs, ROPAs or DPIAs), more advanced metrics display *trends* (e.g., average time to respond to DSRs over time; supplier assessments performed over time). Ultimately, metrics are used to drive or show *outcomes* (e.g., mitigation of privacy risks; comprehensiveness of data mapping; sales won with privacy review).

The next part presents various strategies privacy leaders use to weave privacy metrics into a narrative in order to advance program goals, such as increasing resources and awareness, ensuring organizational support, and enhancing trust.

Privacy Metrics in Action

Members of the FPF Privacy Metrics Working Group presented various ways to demonstrate the strategic value of privacy initiatives, shifting from activity based key performance or risk indicators (KPIs/KRIs) to metrics advancing business value. While *compliance* and *operational* metrics are the base, more mature privacy programs develop *business imperative* metrics, including both customer focused and business enablement metrics.

Examples of *customer focused* metrics included:

- Increase in personalization (as proxy for trust, which is difficult to measure). Privacy leaders demonstrate an increase in consent rates, consumer opt-in rates or collection of first party data as a measure of better data utilization.
- Privacy Customer Experience (CX) metrics. This includes direct feedback from customers about their privacy experience. For example, privacy leaders could measure consumer satisfaction (CSAT) scores in B2B as well as for B2C interactions (*e.g.,* measuring CSAT for user queries by using a thumbs up/down button).
- A/B testing on privacy messaging and language. Privacy leaders conduct focus groups to assess user interface, experience, and satisfaction.
- Competitive benchmarking. Privacy leaders compare indicators against competitors; including, for example, number of cookies by purpose; security certifications; last update of privacy policy; company PR relating to privacy/security; and more.

Examples of *business enablement* metrics included:

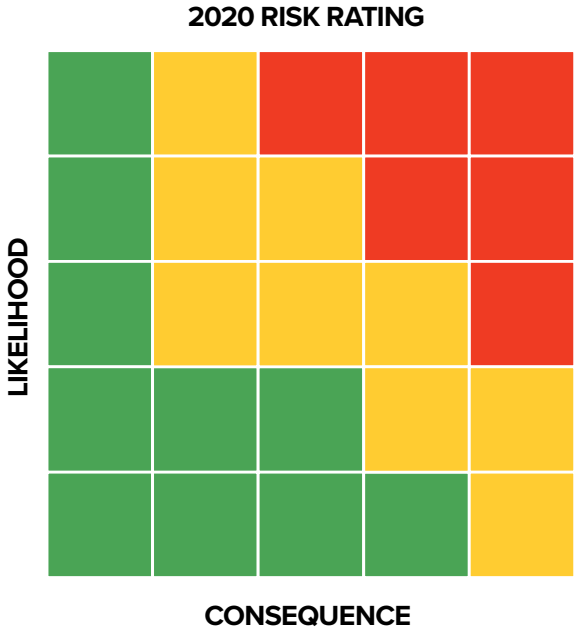
- Privacy as a competitive differentiator. Privacy leaders measure the effect of designing privacy into products and features; enabling greater freedom with data use and innovation.
- Increased win rate (sales). Privacy leaders measure the number of sales calls which include privacy representatives as well as the "win" rate for calls with or without privacy representatives. Privacy leaders count deals closed where privacy was a key negotiation point.
- Faster business processes. Privacy leaders measure the speed of response to inbound vendor questionnaires, completion of due diligence by prospects, sales cycle, etc.
- Operational excellence metrics. Privacy leaders demonstrate time efficiencies in conducting privacy and data protection impact assessments, transfer impact assessments and vendor assessments as well as for negotiating data processing agreements.
- Privacy Employee Experience (EX) metrics. Privacy leaders demonstrate greater employee satisfaction and loyalty given enhanced trust, including increased eNPS (employee net promoter scores).

Risk Management

Members of the FPF Privacy Metrics Working Group discussed using privacy metrics as part of a risk management strategy. Where privacy metrics are considered Key Risk Indicators (KRI) they are reported in a more formal manner, including possibly to the board audit or risk committee. Once recognized as a source of risk, privacy meets the discipline of risk management, which uses quantitative analysis to measure reputational, operational, financial, security, and legal risks. Members recognized the difficulty of introducing the contextual and nuanced concept of privacy into quantitative risk management frameworks. By using metrics, privacy leaders can better assess, manage, mitigate, and present risk factors such as:

- legal and regulatory risks (*e.g.*, compliance with new laws and regulations, changes introduced by the *Schrems II* case)
- technology risks (*e.g.*, increased use of customer collaboration tools, migration to cloud)
- vulnerabilities and threats (*e.g.*, cyber threats, incident history and trends)
- changes to business environment and processes (*e.g.*, expansion to overseas markets, COVID-19 related digital transformation)
- reputational risks (*e.g.*, negative media coverage, possible impact on share price)
- industry standards and best practices (*e.g.*, ISO, NIST, PCI/DSS)

One member demonstrated the use of a two-by-two graphic for assessing privacy risks in various vectors and tracking their mitigation over time, as a measure of performance of privacy teams:



Benchmarking and Maturity Models

Privacy leaders use metrics to compare their privacy programs to benchmarks and maturity models. According to the *Cisco Survey*, organizations with more mature privacy practices realize greater business benefits from privacy practices than those less mature. Moreover, mature privacy organizations are better equipped to handle changing privacy requirements around the globe. Of course, the maturity of a privacy program also depends on an organization's overall maturity, which affects the type and volume of data processed, size of privacy team, existence of a CPO, etc.

- *Early* stage programs focus on compliance with laws and regulations, real time response to inquiries and incidents, and establishing privacy operations.
- *Mid-level* programs seek efficiencies in automating processes, meeting SLAs, responding to DSRs, incidents and requests, supporting additional business functions and becoming more proactive, for example, through privacy by design.
- *Mature* privacy programs eye higher standards and leverage privacy for strategic goals including customer trust and business enablement. Organizations with mature privacy practices secure increased business benefits and are better equipped to handle new and evolving privacy regulations around the world, including by deploying public policy and government relations expertise. Mature programs are sometimes able to integrate and overlay business metrics onto privacy metrics.

Members use privacy metrics to benchmark their programs across industries and jurisdictions. As a basis for benchmarking they use:

- Legal frameworks such as:
  - OECD Privacy Principles
  - APEC Privacy Principles
  - GDPR (and UK DPA)
  - US federal legislation (HIPAA, GLBA, COPPA, FCRA, VPPA)
  - US state legislation (CCPA, CPRA, CDPA, BIPA)
  - LGPD (Brazil), PIPEDA (Canada), Privacy Act (Australia & New Zealand), PIPA (South Korea), etc.
- Standards such as:
  - AICPA GAPP
  - NIST Privacy Framework v2
  - ISO (27001, 27018, 27701, 29100, ISO/PC317)
- Industry frameworks such as:
  - TrustArc-Nymity Privacy Management Integrated Framework
  - CIPL Accountability Wheel
  - IAPP Governance Report
  - IAPP DPO Report
- Custom/Private frameworks
- Collaborative (peer) benchmarking

Members of the FPF Privacy Metrics Working Group reported using metrics to identify and act on opportunities to enhance privacy management processes and deepen program maturity.

Tools and Automation

Members of the FPF Privacy Metrics Working Group discussed various technologies and tools they deploy to collect, assemble, maintain, count, and analyze data for privacy metrics. They agreed that the key to creating a robust privacy metrics system is a shift from manual processes to ticketing systems and other tools with automated collection and processing of data for metrics. Tools range from commonly used platforms such as email and intranet to enterprise software, Governance, Risk and Compliance (GRC) solutions such as ServiceNow or RSA Archer, and dedicated privacy tools. Tools for collecting, maintaining, and presenting privacy metrics include:

- Automated Privacy Governance Controls and Processes
- Privacy Mailbox
- Privacy Intranet
- Privacy module on enterprise software. (*e.g.*, setting up FAQs on privacy, instances to log privacy tickets, number of contracts, value of contracts)
- Privacy GRC Tools
- Privacy software tools (*e.g.*, tools for tracking DSR requests/fulfillment, retention, policy management and violation)

Conclusion

Privacy leaders use metrics for purposes ranging from demonstrating and documenting compliance to asserting the value of their privacy program for data governance, risk management, business enablement, and customer trust. Metrics range from activity based to outcome focused; distinguish between early stage and mature programs; help benchmark against industry standards or competitors' practices; and facilitate risk management and mitigation. Privacy leaders leverage metrics to communicate with internal stakeholders, ranging from employees to senior management and the board, as well as with external parties, including customers, consumers, investors, regulators, advocates, and the media. This report provides a snapshot of the privacy metrics programs and strategies deployed by industry leaders at the FPF Privacy Metrics Working Group. Additional work will focus on case studies demonstrating how group members use metrics in various real-world situations.

Glossary

CSAT: Consumer satisfaction

DPIA: Data protection impact assessment

DSR: Data subject request

ESG: Environmental Social Governance

GAPP: Generally Accepted Privacy Principles

PIA: Privacy impact assessment

PIMS: Personal Information Management Systems

ROPA: Record of processing activities

SLA: Service Level Agreement(s)

1350 EYE STREET NW, SUITE 350 | WASHINGTON, DC 20005 INFO@FPF.ORG