Innovations in the marketplace have accelerated sharply, and the implications have tremendous impact on the business environment. Needless to say, organizations are evolving in scale and geographical outreach that have not been witnessed before. Transforming business frontiers have created an expanding digital universe and explosive data growth, making organizations reservoirs and refineries of data. An analysis by the International Data Corporation (IDC) estimated that by 2020, the digital universe will contain nearly as many digital bits as there are stars in the physical universe.1 Put another way, data are doubling in size every two years and, by 2020, the digital universe is expected to grow exponentially, reaching 44 zettabytes. In all likelihood, this trend will continue and intensify in magnitude. It is widely argued that new economies based on data as a form of capital, and the most coveted strategic asset, will emerge. Data such as personally identifiable information (PII), trade secrets and intellectual property (IP) free flow across organizations, reflecting lowered barriers to data movements and a decline in what consumers refer to as a “privacy friendly” environment. A typical data life cycle and possible interactions with different supply chain relationships are depicted in figure 1.

The fading organizational boundaries, along with increasing appreciation of cloud-based networks, big data, persistent online lifestyle, and comingling of social and business data, create potentially far-reaching privacy and data protection implications. Covert attacks and information theft by perpetrators and criminal cartels are redefining present-day norms. In many respects, the organizational digital doctrine emulates the natural history metaphor, “the struggle for privacy and survival of the secured,”2 which is why data are both an asset and a liability.

The fragmented approaches and pointed solutions that organizations routinely accept to manage their operations and the underpinning data transactions have fallen short of addressing the consumer’s right to privacy. At the same time, the silo approach to privacy has prevailed for far too long without benefit, and organizations are overdue for a paradigm shift to an enterprisewide pursuit to privacy. The enterprisewide pursuit embarks on integrating privacy and protection safeguards into products/systems/services from the earliest stages of design through the privacy-by-design paradigm.

**What to Expect of Privacy by Design**

Identifying, assessing and promoting sound privacy and data protection baselines are crucial for good supervisory practices. Leading practices, industry

---

**Sudhakar Sathiyamurthy, CISA, CRISC, CGEIT, CIPP, ITIL Expert**

Is a director with Grant Thornton’s risk advisory services, focusing on cyber risk. His experience has been shaped by the opportunity to help clients design and implement strategies to achieve a risk intelligent posture. Sathiyamurthy frequently advises clients on standing up and scaling cyber security and privacy capabilities and benchmarking them against laws, regulations, leading practices and industry standards. Sathiyamurthy has contributed to various cyberrisk innovation efforts and authored opinions and articles for leading journals. He can be contacted at sudsathiyam@gmail.com.
standards, corporate binding rules, and national/international laws and regulations set the baseline for privacy and data protection frameworks. The 2014 ISACA® Privacy Survey reveals that International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, COBIT®, EU Directive 95/46/EC, American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA) Generally Accepted Privacy Principles (GAPP), and US National Institute of Standards and Technology Special Publication SP 800-53 are the most commonly used frameworks for managing privacy. The European Union General Data Protection Regulation (GDPR) explicitly embraces privacy and data protection by design as a legal obligation. The illustration in figure 2 shows the themes embraced by the common privacy and data protection frameworks.

Multiple factors drive the need for a defensible privacy-by-design notion, and a representative list of themes is referred to in figure 3.

However, setting up a leading-edge program of privacy by design is often challenged by the following illustrative shortcomings:

- **Nonhomogeneity of laws and regulations**—With an uneven playing field created by the enactment of national and international privacy laws and regulations, instilling a common privacy denominator into engineering practices is not straightforward.

- **Misconceptions of data**—The misconceptions and human biases that shape the value system around the types of data (such as physical identity, social identity, genetic identity, health and wellness identity) and their sensitivities vary across nations. With a uniform definition of personal information not set in stone, changing privacy to suit individual expectations is perceived as a moving target.

- **Legacy solutions are beyond repair to integrate privacy**—Legacy solutions are not only poorly suited to address the emerging class of privacy risk, but are also overstrained with incremental repairs to fit privacy and data protection gaps.

- **Time-to-market overshadows privacy**—Products and solutions are sometimes rushed to market for competitive reasons without considerable thought to privacy implications. Organizations tend to balance privacy design requirements against business objectives and often care less about privacy demands.

- **Disarray due to competing priorities**—Product and solution design encompasses multiple interests and expertise and, hence, creates competing priorities of disparate parties (e.g.,
• Institutional knowledge of personal data elements and data flow is limited—Data protection safeguards are contingent on institutional knowledge and visibility of data elements and their flow, which, in many cases, are not fully mature.

Business discomfort with privacy engineering principles—Businesses that seek to monetize personal data (such as for online behavioral advertising) are sometimes uneasy with being inhibited to collect and use data if privacy engineering principles are implemented.
based on fluctuations in privacy rule sets. Privacy generally is not the primary requirement of a product/system/service build-out, and it is not unusual for privacy requirements to conflict with functional requirements. Sometimes, deploying privacy by design limits the functionalities of the resulting solution. As a result, a trade-off between privacy and business value should be reviewed sensibly within the constraints of the agreed-upon purposes.

With privacy and data protection constituting the core values of the user community, there have been debates on embedding privacy and data protection principles into products/systems/services from the beginning of the design process. While the genesis of privacy by design has made its way beyond debate, tangible engineering strategies still remain unclear for many organizations. The privacy-by-design paradigm can be achieved by aligning it to the core principles illustrated using blockchain technology; an example is shown in figure 5.

Blockchain, in a nutshell, is a combination of protocols and technologies that create a distributed, consensus-driven database, which enables trusted transactions and data exchanges between parties without the need for arbitrators to mediate the exchange. Transactions on a blockchain are not regulated by any central authority. The entities and/or individuals involved in a given transaction provide their information (including personal information), which is then verified by nodes in the network (also known as miners). In this sense, the users forming the community act as their own authorities in a blockchain.

In light of these shortcomings, privacy by design does not happen automatically; it needs to be promoted through integration with organizational influences, such as the enterprise’s culture and belief system.

How to Achieve Privacy by Design

In a real-world scenario, integrating privacy requirements into products/systems/services is not straightforward. The significance of data flow within the product/system/service is illustrated using the analogy shown in figure 4. A typical information system makes quantum connections with neighboring systems, and the chain of connections extends to related systems across the organization and its supply chain constituents.

Privacy by design is multifaceted and can require reordering of priorities or reevaluation of assumptions...
Entity X initiates a transaction with Entity Y.

Miners verify and confirm legitimacy of transaction in publicly available ledger.

New block is added to the blockchain.

Transaction is fulfilled.

- The digital trails associated with blockchain transactions and the metadata of personal details may still be sufficient to expose personal data and reveal private information about people. The exposure of metadata may have an upsetting impact on privacy.

- The distributed nature of transactions in the blockchain is recorded on a publicly available ledger and renders the transactions processed unalterable. This transparent and immutable nature of blockchain may raise issues as user’s
As new blockchain use cases emerge rapidly, ensuring defensible design of blockchain technology that accounts for user privacy and data protection is the key.

The following principles set the tone for privacy by design relative to blockchain technologies:

- **Proactive not reactive; preventive not remedial**—Frequently, amends for infringements of privacy and data protection obligations are usually reactive, taking effect only after the fact. In a complex distributed blockchain ecosystem, systematic monitoring and trustworthy functioning is critical to proactively sense nonconformities. Given that there are not many industry standards and regulations to govern the blockchain ecosystem and considering the potential risk that could undermine the privacy of transactions, this principle aims to prevent events that compromise users’ privacy before they happen and not after the privacy risk materializes.

- **Right-sized privacy**—This principle seeks to deliver a reasonable degree of privacy by ensuring that personal information (such as financial and digital medical records) transacted in the blockchain is protected by appropriate technical and organizational measures.

- **Privacy protection embedded into design**—A typical engineering process focuses on realizing the functional requirements of the solution, and privacy and data protection assurances fall short as a result. These shortcomings are exacerbated by challenges associated with engineering privacy. This principle seeks to consider privacy needs from the very beginning of the engineering process. The viability of blockchain depends on its ability to deliver a privacy and data protection promise. The blockchain engineering process should be supported by appropriate libraries of privacy design strategies and privacy-friendly solutions to help designers support and realize a user’s right to privacy.

- **Full functionality; positive-sum, not zero-sum**—This principle seeks to accommodate the legitimate interests and objectives of the individuals whose data are at stake in a positive-sum, “win-win” manner. An optimal blockchain strategy should account for solution value drivers, current opportunities, challenges and limits of the privacy-by-design principles and describe ways to ensure trustworthy functioning.

- **End-to-end security; full life cycle protection**—Confidentiality, integrity and availability considerations provide guidance on secure design choices and appropriate safeguards for privacy and data protection. Security considerations should follow the data wherever they go (from collection, storage, use, transfer, destruction) and protect blockchain technologies against malicious adversaries and cyberattacks.

- **Visibility and transparency; keep it open**—Visibility and transparency are related to the principles concerning openness. This principle seeks to assure stakeholders that blockchain services operate according to the stated promises and objectives subject to independent verification. While regulations and leading practices designed to standardize blockchain transactions could prove beneficial, independent auditing and verification
methods can provide reasonable oversight until regulatory and legal precedents catch up.

• **Respect for user privacy; keep it user-centric**—Traditional engineering design practices barely consider the privacy and data protection interests of end users. This principle seeks to rationalize and account for the interests of all parties involved in blockchain solutions and services by offering creative countermeasures and privacy-friendly solutions.

The aforementioned principles set the minimum baseline for achieving privacy by design, however, these principles are not by themselves an absolute guarantee that the product/system/service will comply with all privacy requirements. The privacy-by-design approach is a continuous process and, therefore, compliance to privacy mandates should be continually reviewed in perspective of changes and/or updates to national and international privacy laws and regulations.

### Conclusion

New generations of consumers have behaviors and expectations that drive privacy-friendly versions of current products, systems and services. Legal, regulatory requirements and social practices help enlighten to better respond to consumer demands and better inform privacy-by-design solutions. The confluence of these powerful forces is a compelling driver of the need for consumer privacy improvements.

The genesis of privacy is to protect users’ rights and their freedom to determine how personal information is used, which is why privacy by design is a stride toward consumer-centric design. Consumer-centric design does not operate in a “building products by techies for techies” manner. Instead, it focuses on transparent and trustworthy design that empowers users to exercise their right to and over information.

In the aggregate, institutional improvements must operate in ways that allow for the highest possible measure of consumer trust. Smart organizations will not resist this trend. They will underscore the importance of creating a privacy-friendly ecosystem and fostering privacy by design.

### Endnotes


6. American Institute of Certified Public Accountants (AICPA), *Generally Accepted Privacy Principles (GAPP)*, USA

