Privacy Compliance—A Path to Increase Trust in Technology

The need for privacy is increasing at an unprecedented rate. It cuts across technologies and work models, especially the new ones, that create opportunities for and facilitate the management of personally identifiable information (PII). The key goal of privacy is to earn the trust of the data subjects. In earning this trust, regulatory requirements provide the threshold of what is necessary. This can be systematically achieved through approaches discussed in the Privacy Frameworks, Standards and Best Practices section herein.

Why Privacy Matters

It is important to understand what is meant by privacy. According to the ISACA® glossary, privacy is defined as:

> *The rights of an individual to trust that others will appropriately and respectfully use, store, share, and dispose of their associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived.*[1]

Privacy implies that an individual has complete control over their personal information during the entire life cycle of data including receipt, generation, processing, sharing, storage and deletion. At least three parties are involved in the privacy space: data subject, data controller and policymakers. Most discussion on privacy is from the viewpoint of the data subject.

More personal information about an individual could provide potentially more opportunities to organizations to use it for various commercial purposes, e.g., to influence an individual's buying pattern and commercial decisions. However, personal information in the wrong hands can cause financial and reputational loss; hence, maintaining the privacy of personal information is gaining recognition as critically important, especially in the current era of digital transformation. Implementation of information

Vasant Raval, DBA, CISA, ACMA
Is professor emeritus of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and financial fraud. He recently published a book on corporate governance. He can be reached at vraval@creighton.edu.

Samir Shah, CISA, ACA, CFE, CIA, CIPM, CISSP
Is an associate partner with the Business Consulting Services of Ernst & Young. He has more than 20 years of progressive management experience with a focus on the banking and financial services vertical. He has worked extensively on various dimensions of risk, audit and privacy. He can be reached at samirnshahca@gmail.com.

security enables required protection to all enterprise information assets, including personal information. Trust in technology is enhanced by effective implementation of information security and by complying with the information privacy requirements of applicable regulations and data subject mandates.

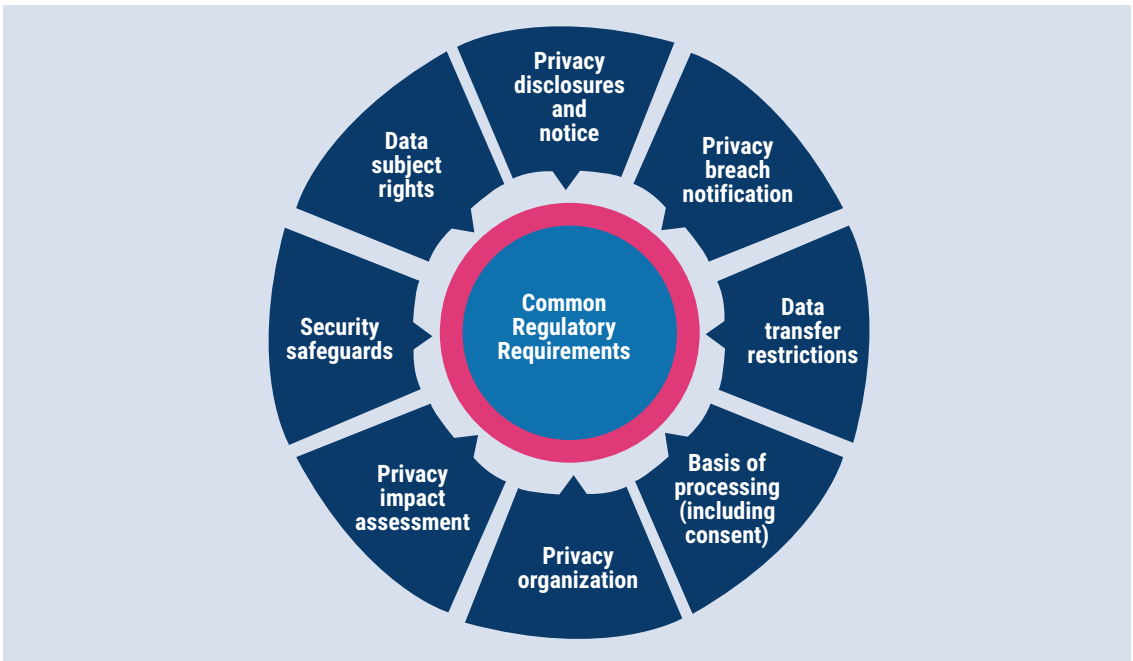
Privacy Regulations Worldwide

Generally classified under eight themes (**figure 1**), privacy statutory and regulatory requirements have been around at least since the early 1980s. However, such requirements could not be effectively implemented due to relatively weak enforcement for noncompliance. This changed when regionally enforceable requirements were sought out. For example, the EU General Data Protection Regulation (GDPR), effective May 2018, was launched in Europe with stringent penalties for noncompliance. Many other countries including Bahrain (Personal Data Protection Law), Brazil (Lei Geral de Proteção de Dados [LGPD]), New Zealand (The Privacy Act 2020), Thailand (Personal Data Protection Act) and the United States (California Consumer Privacy Act [CCPA]) have also enacted detailed and stringent personal data protection laws. The generic aim reflected in these regulations is to increase transparency through privacy notice and consent, empower data subjects through various rights (e.g., access, rectification, erasure, portability, object to specific processing), provide timely communication of data breaches, and enable better risk management and governance of the personal information through privacy impact assessment and the establishing of a privacy organization. However, this raises an interesting question: If the end-goal is the same, are so many blueprints to regulate privacy necessary?

> "DATA CONTROLLERS CAN ONLY RECEIVE THE TRUST OF THE DATA SUBJECTS IF PRIVACY REQUIREMENTS ARE PERCEIVED TO HAVE BEEN ADDRESSED ADEQUATELY."

A few of these regulations also have specific IT-related requirements around cookies and similar online trackers, data anonymization, adoption of privacy by design in the information systems, and more. These regulatory requirements, along with

Figure 1—Common Themes of Regulatory Requirements of Privacy



voluntary adoption of privacy best practices such as data minimization, privacy by default, privacy disclosures, and consent, are contributing significantly to the enhancement of trust in technology.

Privacy is a unique mix of technical and human considerations. Generally, functional requirements that depend on technological capacity are easy to identify and provide for, but the nontechnical attributes may be difficult to design into systems. From a technical requirements perspective, the data controller should consider risk and provide for confidentiality, integrity and availability. From a nontechnical requirements perspective, however, the rights of data subjects—unlinkability, transparency and intervenability—come into play. Data controllers can receive only the trust of the data subjects if privacy requirements are perceived to have been addressed adequately.

Footprints of data and applications can traverse geographies, technologies and applications—to a point where the data subject will not have a good understanding of how well the subject's privacy is guarded. Also, if too much burden is placed on data controllers for privacy-related requirements, they could become indifferent or negligent toward privacy matters. They might wonder: Is privacy for real?

PII cuts across systems, applications, data, communication and more, so the design to meet privacy requirements, both logical and legal, could get quite complicated. Once designed, the need to maintain continued fulfillment of updated requirements poses a constant challenge.

Privacy Frameworks, Standards and Best Practices

There are several frameworks and standards that provide a structured approach to end-to-end privacy compliance. These include the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27701,[2] the Generally Accepted Privacy Principles (GAPP),[3] SOC 2 and SOC 3 reports,[4] the US National Institute of Standards and Technology (NIST) Privacy Framework,[5] the Secure Controls Framework (SCF),[6] and Privacy by Design (PbD).[7] PbD focuses on embedding privacy into the design of systems, processes and functions. PbD has gained prominence due to an increasing need to proactively build privacy at the design stage of new-age technologies and work models.

> "ORGANIZATIONS OPERATING IN MULTIPLE COUNTRIES ARE ALSO DEVELOPING THEIR PRIVACY FRAMEWORKS BY UNIFYING REQUIREMENTS FROM VARIOUS APPLICABLE REGULATIONS AND DESIRED STANDARDS."

Organizations operating in multiple countries are also developing their privacy frameworks by unifying requirements from various applicable regulations and desired standards. Such unified frameworks are built to avoid duplication of efforts in complying with the common requirements of multiple regulations and to identify the incremental requirements of a specific regulation/country. There are efforts in the public domain to create a unified framework covering common regulatory and standards requirements. More such cooperative and open-source efforts will go a long way in building such unified frameworks to simplify and reduce privacy compliance efforts.

New-Age Technologies, Work Models and Information Privacy Issues

The emergence of new-age technologies such as the Internet of Things (IoT) and work models such as bring your own device (BYOD) have posed several concerns on the privacy aspects of personal information processed by such technologies and work models. Some of the common concerns include:

- What personal information is being collected?
- Where and how it will be used?
- Will the individual know whether and with whom it will be shared and what that third party will do with an individual's personal information?

Enjoying this article?

- Read *Privacy: Beyond Compliance*. *www.isaca.org/privacy_beyond_compliance_2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- Will the individual come to know when their data get compromised? How?
- How long will an individual's data be retained/stored?
- Can individuals ask for copies of their data or the correction/deletion/portability of their data?

PbD would help to address some of these common questions within the core technology to ensure proper implementation of privacy requirements regardless of what technology or work model is used. This can be illustrated by discussing privacy-related issues of IoT.

IoT

Usage of IoT is not limited to smart homes, smart assistants, smart cars and smart wearables; it has also entered core commercial operations such as predictive plant maintenance, smart metering, asset tracking, fleet management and many other applications.[8] Hybrid personal and commercial usage models have emerged; for example, fitness trackers

Figure 2—Implementation Details and Application of PbD Foundational Principles

PbD Foundational Principle	Implementation Details of the Foundational Principles	Example of an Implementation of the Foundational Principles in an IoT Device/Application
1. Proactive, not reactive; preventive, not remedial	Preventive controls take preference over detective or corrective controls.	Personal assistants and wearables apply strong encryption and access control over personal data in transit and at rest.
2. Privacy as the default setting	Apply controls that enable privacy as the default configuration.	Applications do not store or share financial information such as credit card data as the default choice for shopping-enabled IoT devices. Enabling storage or sharing of card data needs additional configuration/action on the part of the user.
3. Privacy embedded into design	Privacy is not an add-on functionality but it is integrated with the core functionality and processes.	Weather application on a wearable device shows notification before sharing location of the device and an option to enable/disable sharing of location.
4. Full functionality—positive-sum, not zero-sum	Enabling privacy does not result in an inferior service or downgraded functionality.	Refusal to store financial data such as card information does not result in constraining shopping functionality in the IoT device and application.
5. End-to-end security—full life cycle protection	Personal information is protected at every stage from receipt, generation, sharing, processing, storage, archival and deletion.	Personal information is protected through encryption during the entire life cycle, including storage on the personal assistant and transmission to the central server. Any further analysis of the personal data is performed on an anonymized/pseudonymized version of the data.
6. Visibility and transparency—keep it open	Privacy practices are visible and transparent and, if required, capable of being audited by an independent third party.	A detailed disclosure by the fitness tracker wearable company as to what data are being collected and where they are used, shared and stored. Also, third-party verification of these practices are performed through SOC 2 reports.
7. Respect for user privacy—keep it user-centric	Privacy configurations and options are designed to enhance user ease and convenience.	There should be a just-in-time notification that personal data will be shared with a third party if map services are enabled on a fitness wearable application. Also, there should be periodic notifications to remind the user that the map data are sourced from a third-party service and personal information is being shared with the service provider.

Source: Rosner, G.; E. Kenneally; *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design, Center for Long-Term Cybersecurity,* University of California, Berkeley, USA, 2018, *https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf*

and wearables are being used by wellness companies to encourage better health routines and optimize insurance premiums. Personal data acquisition and processing is at the core of these use cases, and the information gathered by these devices can be sensitive and personal. Maintaining the highest degree of transparency and empowering data subjects with complete control over their data are critical in enhancing trust in IoT technologies.

PbD Implementation in the IoT Space

Incorporating PbD in the development and implementation of new-age technologies and work models will enhance compliance with the privacy requirements. **Figure 2** presents implementation details and application of the PbD foundational principles.

Conclusion

It is very important to understand what constitutes personal information and what are the regulatory requirements related to such personal information. Both the setting of compliance requirements and their implementation are further complicated by the very nature of new technology platforms and models such as IoT, BYOD, data analytics, blockchain and artificial intelligence. Increasingly, the personal nature of human interaction in private and organizational interactions has become significant and is continuously growing. A proactive and disciplined approach should be used in meeting privacy requirements, for example, though PbD or other methodologies. Meeting the fundamental prerequisites of basic privacy mandates would be better served if technologies embrace the privacy challenge at the design stage of the technology itself rather than its applications later on. This way, at least the ecosystem of the technology will provide a solid foundation for ensuring privacy.

Endnotes

1 ISACA® Glossary, Privacy, *https://www.isaca.org/resources/glossary#glossp*

"INCORPORATING PBD IN THE DEVELOPMENT AND IMPLEMENTATION OF NEW-AGE TECHNOLOGIES AND WORK MODELS WILL ENHANCE COMPLIANCE WITH THE PRIVACY REQUIREMENTS."

2 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27701:2019 *Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines*, Switzerland, 2019, *https://www.iso.org/standard/71670.html*

3 American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants, *Generally Accepted Privacy Principles (GAPP),* USA, August 2009, *https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/00250-generally-accepted-privacy-principles.pdf?la=en*

4 American Institute of Certified Public Accountants (AICPA), SOC 2—SOC for Service Organizations: Trust Services Criteria, USA, *https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html*

5 National Institute of Standards and Technology, (NIST), *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0*, USA, 16 January 2020, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf*

6 Secure Controls Framework (SCF), SCF Privacy Management Principles, *https://www.securecontrolsframework.com/privacy-management-principles*

7 Cavoukian, A.; *Privacy by Design: The 7 Foundational Principles*, Canada, 2011, *https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf*

8 Tracy, P.; "The Top 5 Industrial IoT Use Cases," IBM, 19 April 2017, *https://www.ibm.com/blogs/internet-of-things/top-5-industrial-iot-use-cases/*