Need a deeper dive on this topic? **Ask-An-Expert**

Infosec in 2019: What to Expect in Privacy Regulations/Legislation

November 27, 2018 | Faculty Reports | Privacy | By Rebecca Herold, IANS Faculty

Executive Summary

For the past few decades, organizations have been struggling with how to better protect personal data, while trying to comply with the growing number of legal requirements for using and managing it. Regulations are now being enacted that go beyond specific industries, technologies and personal data items. And this means all organizations, in all industries, need to prepare for 2019 by establishing a comprehensive privacy management program to address the additional and expanded privacy requirements set to emerge in the next year and beyond.

In this report, we explain how we got here, how privacy regulations and legislation evolved and the implications of new privacy regulations such as the EU’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). We also detail what we expect to see in terms of privacy/compliance issues in 2019 and provide a detailed 10-step plan for meeting those challenges by establishing and maintaining a strong privacy management program that will serve and protect your organization – not only in 2019, but over the long term.

Patchwork Laws Start the Trend

Privacy standards, laws, regulations and other types of legal requirements are emerging worldwide to address a wide range of privacy issues, and they include a vast range of differing requirements. What brought us to this point?

While privacy laws and regulations generally emerged early in the U.S. compared to other countries, they either tended to address specific types of personal data or applied only to specific industries, and often in limited ways. Consider the following brief and incomplete history of legal protections for privacy evolution within the U.S. in the past century:

- **Tort law**. These laws emerged during the first half of the 1900s, but they did not cover explicitly named personal data items and were not applicable only to specific industries. They related to the invasion of privacy to individuals in general and addressed intrusion of solitude, public disclosure of private facts, placing a person in a “false light” and appropriation. (For a discussion of the four types of tort laws, see "**Privacy**," by William L.

Prosser.)

- **Industry-specific laws, regulations and standards.** Multiple industry-specific regulations, all with different requirements, were enacted in the late '90s and early 2000s. These included the **Health Insurance Portability and Accountability Act** (HIPAA), which applies to healthcare entities, and the **Federal Information Security Modernization Act** (FISMA), which applies to federal government agencies. Possibly the most impactful data security and privacy standard in the U.S. is the **Payment Card Industry Data Security Standard (PCI DSS)**, which must be implemented by all organizations that process credit card payments.

- **Breach notice laws.** Laws requiring organizations to give breach notices to associated victims were born when California enacted **SB1386** in 2002. After this seminal event, states slowly, at first, started implementing their own breach notice laws, each of which were slightly to significantly different than the others. As of this writing, there are now **54 U.S. state and territory breach notice laws**, and they are all still all slightly to significantly different from each other. Since SB1386 (which has been updated), federal regulations including breach notice requirements have also emerged. One example is the **HITECH Act**, which applies to the healthcare industry.

- **Miscellaneous laws**. After the public's widespread welcome of the breach notice laws, many other state laws, federal regulations and industry standards targeting specific types of situations and technologies involving personal data were implemented. Encryption requirement laws, credit freeze laws, laws requiring specific controls for explicitly named technologies, regulations establishing specific requirements for handling personal data, as well as third-party access to smart meter-based information standards and data protection principles for connected vehicles (to name just a few) all appeared. There are literally hundreds more that could be listed (see a long list published by ISACA **here**).

All these laws, regulations, standards and guidelines often overlap, have contradictory requirements, sometimes dovetail and almost always result in a crazy quilt type of privacy management program that organizations struggle to keep patched together to ensure not only effective personal data protections, but also to provide due diligence for compliance with all applicable legal requirements.

GDPR Jolts Organizations into Action

While U.S-based organizations were grappling with identifying and then figuring out how to comply with all the applicable privacy laws, regulations and standards, the European Union (EU) undertook an initiative, starting around 2011, to replace its long-standing Directive 95/46/EC with a more effective, comprehensive and prescriptive personal data protection regulation (for more, see **The History of the General Data Protection Regulation**). The result was GDPR, which was approved in 2016 and went into effect **on May 25, 2018**.

When GDPR gained approval, most worldwide privacy advocacy groups were elated. Most EU data protection professionals and organizations hailed it as the long-overdue establishment of privacy rights that all organizations throughout the world would now be compelled to or should follow in one way or another, sooner or not-so-much-later.

However, most U.S.-based businesses were confused; they did not know if or how the extraterritorial and highly detailed requirements within GDPR would apply to them. Lawsuits against U.S.-based entities were filed **on the first day GDPR went into effect**. Then, almost one month to the day following the GDPR effective date, on June 28, 2018, **CCPA** was signed into law. While applicability of CCPA is not as broad as GDPR, the concepts within it closely mirror GDPR.

Now that California has created its own GDPR-like law, many other states are also considering implementing their own versions as well. And there are increasing calls from lawmakers, privacy rights advocates and the general public for Congress to enact a comprehensive privacy law at the federal level to protect **all types of personal data, within all types of organizations**.

This has left many organizations wondering what requirements in GDPR and CCPA are unique and not already within existing laws that U.S.-based organizations have already been addressing.

Rundown of New Requirements

Key requirements within GDPR and CCPA that were not to date explicitly covered within that patchwork of hundreds of other laws and regulations include, at a high level, the following rights for individuals (i.e., "data subjects"):

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Along with these rights provided to individuals, GDPR and CCPA bring two other significant requirements. Organizations (i.e., "data controllers") must now:

- **Consider the likelihood and severity of impact on individuals** when considering risks involved with personal data. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- **Use a broader definition of "personal data."** The definition is now widened to include any data that can **directly or indirectly identify an individual**. This includes many more possible information items, within many more contexts, than the delimited, specifically named information items found in most other established state and federal privacy laws.

What to Expect Near-Term

In 2019 and 2020, organizations should expect to see more:

- **Tech companies promoting their own versions of privacy regulations** in the hopes that lawmakers will enshrine them into law. **Google**, **Apple** and **Intel** each published their own proposed privacy bills and frameworks. Although they all differ in requirements, they are similar in that they generally advocate establishing one set of requirements for all organizations in the U.S. to use, instead of the current business environment, which includes hundreds of laws and regulations with often conflicting requirements.
- **State-level privacy laws.** States will enact laws for specific types of requirements for specific types of technologies and personal data, in addition to implementing their own more comprehensive privacy protection requirements, similar to CCPA and GDPR.

- **Guidance coming from regulators enforcing GDPR and CCPA.** As organizations make the challenges with implementing GDPR requirements known to data protection authorities (DPAs), and as DPAs do more investigations for non-compliance, they will take the associated lessons learned and incorporate them into guidance documents. Other organizations would be wise to read and then act on this guidance if the issues covered are also present within their own enterprises.

- **Industry standards.** Industry groups and lobbyists are scrambling to try and establish their own industry privacy standards to use for self-regulation to prevent as many federal regulations from being enacted as possible. This tactic has had mixed success in the past. It will be interesting to see how successful it will be going forward with more lawmakers and tech giants jumping on the federal privacy regulation promotion train.

- **Fines and penalties, and more of them applied, for non-compliance with existing rules.** HIPAA non-compliance fines have steadily increased over the years, and GDPR is already embracing high penalties from the get-go.

- **Organizations requiring vendors and other contracted entities to prove they comply** with the wide range of privacy legal requirements. Organizations have been burned with fines and brand damage from breaches and non-compliance of their contracted third parties. They are finally, and justifiably, being more proactive to ensure the data they entrust to third parties is appropriately safeguarded and used.

10 Steps to Get Ahead of the Curve

When it comes to compliance, many organizations try to dig right in and go straight to addressing each of the requirements, one at a time, within each of their applicable legal obligations. However, such a tactic is not only time-consuming, inefficient and likely to result in compliance gaps, it is also usually futile.

Instead, as we enter the new year, organizations must address privacy holistically within an effective and comprehensive privacy management program that establishes the framework around which privacy practices will be implemented within the enterprise.

The following 10 steps can help jumpstart an organization’s privacy management program, while at the same time enable it to support multiple privacy legal requirements.

1: Create a Role Responsible for Privacy Management Within the Enterprise

Organizations must establish (and create a clearly written description for) a role with overall responsibility for the enterprise privacy management program.

This role should be visibly and strongly supported by executive management, and there should also be written descriptions for the roles that have accountability for performing privacy management activities.

2: Determine Specific Legal Requirements Around Privacy

Organizations must determine and document applicable legal requirements (laws, regulations, standards and contracts) for identified personal data. This is important for a couple of reasons:

- **You can’t manage what you don’t know.** A large portion of privacy work involves consideration of organization-applicable legal requirements. There is also a need to reference specific legal requirements when considering what to include in an effective privacy management program.

- **Privacy managers require guidance.** Establishing such a catalog of applicable legal requirements is critical for individuals managing the privacy program. This allows them to monitor those specific requirements on an ongoing basis, and enables them to identify any changes in applicable laws and adjust the privacy program policies and procedures.

3: Define Key Terms

Organizations must clearly communicate the meaning of key terms within a privacy management program to ensure everyone involved understands the terms in the same way and everyone throughout the enterprise is on the same page. If this is not accomplished, privacy cannot be managed successfully, much less consistently, throughout the organization.

For example, some organizations prefer to use the term “personal information” (the term used in CCPA) to better convey the notion that the term applies to all forms of information, such as audible, visual, hard copy, etc., and not just to digital data. Other organizations choose “personal data,” since that is the term used within GDPR. Each organization should decide which term is best for their own business environment, define it as it applied to the organization, and then use it consistently within their privacy management program communications and documentation.

Two key terms that every organization should include within their privacy management program are:

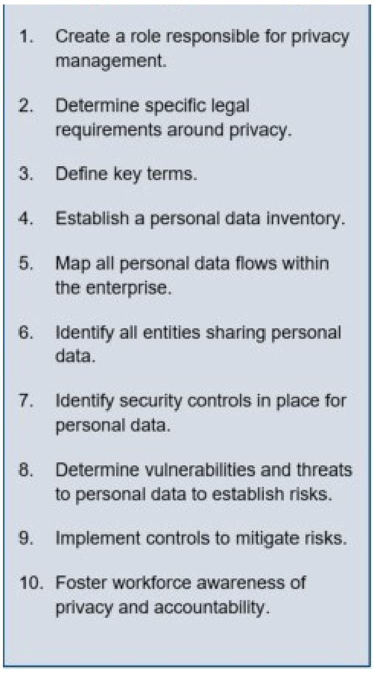
- **Privacy**. A universally accepted definition for “privacy” does not exist. It is a largely subjective term, for which each organization must establish its own definition to be consistently considered and applied throughout the enterprise. When establishing this definition, organizations must consider the context of the situations within which personal data is being collected, used, stored or otherwise accessed, as well as the rights, values and interests of individuals. The related characteristics, descriptive information and labels, activities and opinions of individuals are just a few of the applicable privacy considerations. Privacy means many things to different individuals, depending on a variety of historical, social, cultural and political factors. Privacy also has different meanings for different enterprises and governments, and to nonprofit and global associations such as ISACA throughout the world. At its most rudimentary and long-standing definition, privacy can be the right to be left alone. **ISACA’s comprehensive, internationally inclusive definition** of privacy is:

  > “The rights of an individual to trust that others will appropriately and respectfully collect, use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived. What is appropriate depends on the associated circumstances, laws and the individual’s reasonable expectations. An individual also has the right to reasonably control and be aware of the collection, use and disclosure of his/her associated personal and sensitive information.”

- **Personal data**. One common thread throughout these laws, regulations and standards is that personal information, or information that can be linked to a specific individual, is involved in one or more ways. Each organization needs to perform an analysis to determine all the different types of information that could be linked to an individual, or groups of individuals, and establish their own definition based on the results of analysis. Use this also to establish your personal data inventory, if you’ve not yet established one. If your organization has such an inventory, the results of analysis can be used to update that inventory with any personal data items that are missing. (For help with this analysis, see IANS’ **Personal Data Inventory Worksheet**.)

Other terms should be established based on the applicable legal requirements, business environment, locations for consumers/customers and workers, and other factors.

4: Establish a Personal Data Inventory



1. Create a role responsible for privacy management.
2. Determine specific legal requirements around privacy.
3. Define key terms.
4. Establish a personal data inventory.
5. Map all personal data flows within the enterprise.
6. Identify all entities sharing personal data.
7. Identify security controls in place for personal data.
8. Determine vulnerabilities and threats to personal data to establish risks.
9. Implement controls to mitigate risks.
10. Foster workforce awareness of privacy and accountability.

Once the key terms for the privacy management program have been established, an inventory of personal data should be established and kept up to date.

When establishing the personal data inventory, involved key stakeholders throughout all the business units should discuss all the types of information they collect, process, store, share and otherwise handle within their areas to ensure key personal data items are not overlooked.

5: Map All Personal Data Flows Within the Enterprise

Once the organization determines the types of personal data it has, it's time to identify where the personal data is collected, accessed, stored and shared. This helps organizations identify the associated security and privacy controls involved and then determine any existing associated data security and privacy risks. (For help with mapping data flows, see IANS' **Personal Data Flows Worksheet**.)

6: Identify All Entities Sharing Personal Data

Organizations must identify all entities sharing personal data – within and outside the organization. This is necessary to determine all parties with access to the personal data, which in turn helps support many privacy management program activities, such as determining:

- Who is directly accountable for following privacy policies.
- Where procedures need to be established within each area of the organization for the associated job activities involving personal data.
- The most appropriate types of security and privacy tools to use throughout the data flows.
- The best way to establish third-party security and privacy oversight.

The **Personal Data Flows Worksheet** can also help with this step.

7: Identify Security Controls in Place for Personal Data

By identifying the full data-flow lifecycle, the associated security controls throughout the data flows can be identified. This includes determination of the methods and applications used to transmit the data, as well as the associated security controls used throughout, such as encryption and virtual private network (VPN) tunnels, or where no security controls are used.

8: Determine Vulnerabilities and Threats to Personal Data to Establish Risks

Detailed data-flow maps allow organizations to more clearly and quickly identify vulnerabilities to personal data (such as when personal data passes through public Wi-Fi networks in clear text) and threats to data (such as all the users of the public Wi-Fi network who are not authorized to access the organization's data). These insights will support more efficient data security risk assessments and privacy impact assessments.

9: Implement Controls to Mitigate Risks

Fully mapped personal data flows, with identified risks, enable identification of the most effective and feasible security and privacy controls to implement to reduce data security and privacy risks to acceptable levels. Plans for controls implementation can then be created with key stakeholders throughout the enterprise.

10: Foster Workforce Awareness of Privacy and Accountability

Organizations must establish and implement or update existing enterprise data security and privacy policies. Work with each business unit and corporate support area to create work-specific procedures for each associated area to support compliance with the established policies. Then make sure all workforce members whose job responsibilities involve access in any way to personal data know and understand the policies and associated procedures, and that they receive periodic, updated training, along with frequent security and privacy reminders relevant to their job activities.

Plan Now for 2019 and Beyond

Ultimately, organizations must understand the need for establishing a privacy management program, even if laws and regulations are not yet imposing requirements on them. Every enterprise that collects, stores, processes or accesses personal data must establish the meaning of “privacy” for their enterprise, employees, customers, patients and all others whose personal information is used in some way.

In addition, each enterprise must also understand how those associated individuals view privacy:

- Within their own culture and associated geographic areas.
- Across geographic areas due to international trade and commerce.
- As defined by applicable laws and regulations.

Organizations that start planning, and then implementing, a comprehensive privacy management program now will be best prepared to meet the inevitable comprehensive personal data protection regulation we expect to see established in the U.S. in the 2019-20 time frame.

Any views or opinions presented in this document are solely those of the Faculty and do not necessarily represent the views and opinions of IANS. Although reasonable efforts will be made to ensure the completeness and accuracy of the information contained in our written reports, no liability can be accepted by IANS or our Faculty members for the results of any actions taken by the client in connection with such information, opinions, or advice.