Wearables and Big Data and Drones, Oh My!
How to Manage Privacy Risk in the Use of Newer Technologies

Julie S. McEwen, CISSP, PMP, CIPP/G/US, CIPM, CIPT

2015 Project Management Symposium, University of Maryland
April 14, 2015

Abstract

Smart energy, unmanned aircraft systems, connected vehicles, wearables, social media, body scanners -- these are all examples of technologies that can collect and/or use personally identifiable information. Privacy continues to be a big concern as new technologies such as these are developed or existing technologies are used in new ways. It has been difficult for privacy methods to keep pace with relevant technological advances. Innovative approaches and tools are needed to properly identify and manage privacy risk. The popularity of the Privacy by Design (PbD) concept reflects this need.

This paper provides a short overview of privacy, including a discussion of the following topics:

- A definition of privacy
- The relationship between privacy and security
- Privacy in the U.S. public and private sectors
- Global privacy perspectives

The paper also discusses what a project manager can do within the project management process to ensure that privacy risk is adequately addressed when managing projects related to technologies that collect and/or use personally identifiable information.
Table of Contents
What is Privacy? .................................................................................................................. 2  
Core Principles of Privacy .................................................................................................. 3  
How Privacy and Security Work Together ........................................................................ 4  
Privacy Harms .................................................................................................................... 5  
Global Privacy Approaches ............................................................................................... 6  
Privacy Engineering ......................................................................................................... 8  
Privacy and Project Management ..................................................................................... 9  
Conclusion .......................................................................................................................... 12  
References ........................................................................................................................... 12

What is Privacy?

Privacy is a very personal concept, and views regarding privacy can vary widely from individual to individual. Privacy definitions also vary across jurisdictions and industries. Privacy is generally defined within the U.S. as the ability of an individual to control the collection, use, and dissemination of his or her personally identifiable information (PII). For U.S. federal government agencies, PII is information that directly or indirectly identifies an individual. The Office of Management and Budget (OMB) has defined PII as:

. . . information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.3

There is no definitive list of PII data elements that applies to all environments. However, PII typically includes identifying information such as name or address, and also includes identifying numbers such as Social Security Number or driver's license number. Examples of PII are provided in the table below.

---

Table 1. Examples of PII

<table>
<thead>
<tr>
<th>Identification Information</th>
<th>Identification Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name</td>
<td>• Social Security Number (or other number created by a government that specifically identifies an individual)</td>
</tr>
<tr>
<td>• Date of birth</td>
<td>• Certificate/license numbers (e.g., Driver’s License Number)</td>
</tr>
<tr>
<td>• Place of birth</td>
<td>• Vehicle Identifiers (e.g., license plates, Vehicle Identification Number)</td>
</tr>
<tr>
<td>• Photographic Identifiers (e.g., photographic image, x-rays, video)</td>
<td>• Passport number</td>
</tr>
<tr>
<td>• Biometric Identifiers (e.g., fingerprint, voiceprint)</td>
<td>• Alien (A-) number</td>
</tr>
<tr>
<td>• Mother’s Maiden Name</td>
<td>• Financial account numbers</td>
</tr>
<tr>
<td>• Mailing Address</td>
<td></td>
</tr>
<tr>
<td>• Phone Numbers (e.g., phone, fax, and cell)</td>
<td></td>
</tr>
</tbody>
</table>

OMB reinforces the idea that PII should be identified on a case-by-case basis, as follows:

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an organization to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.4

Organizations typically must perform an analysis of the data elements that they are collecting, using, sharing, storing, and deleting in order to determine which elements are PII, and also which data elements are sensitive PII within their unique environments. Some PII is always considered sensitive, such as Social Security Numbers. Other PII becomes sensitive depending upon the context in which it is being used. For example, a list of names in a public phone book where the individuals gave their permission for their names to be published is a list of PII that is not considered sensitive. However, the same names appearing on a list of individuals who have a certain medical condition is now sensitive PII since public knowledge of health status can often have negative impacts upon individuals.

Core Principles of Privacy

Privacy is based on the implementation of the Fair Information Practice Principles (FIPPs), which were initially developed in 1973 by a U.S. federal advisory committee. Core privacy concepts based on the FIPPs that are found in privacy frameworks around the world are:

- Notice: Provide clear information about the collection and use of PII
- Limitation: Ensure that minimal PII is collected, used, disclosed, and retained for stated purposes
- Accuracy: Ensure that individuals are treated fairly based on PII that is correct

---

- Choice: Provide individuals with the ability to consent to the collection and use of their PII
- Individual Access and Redress: Provide individuals with the ability to review the PII held about them, correct it, and challenge compliance with stated privacy practices
- Security: Protect against inappropriate access and disclosure and poor integrity of PII

The concept of consent has proven to be especially difficult to implement fully in the electronic world, and there has been increasing attention to the idea that consent should be provided by individuals for information sharing in complex environments such as health care. In some environments, such as law enforcement, the intelligence community, and homeland security, opportunities for choice, access, and redress are often extremely limited. In those environments, providing individuals with the opportunity to provide consent, access information about themselves, and correct that information may also alert them that they are under surveillance or being investigated and result in compromised investigations. Appropriate notice is still required to let the public know in general about activities where government organizations are collecting and using PII.

**How Privacy and Security Work Together**

Privacy and security are two distinct disciplines that are mutually supportive. Security focuses on the use of mechanisms for protecting information and information systems, such as ensuring the availability of systems, malicious code detection and prevention, configuration and patch management, intrusion detection and mitigation, and physical protection. Privacy focuses on the individual's ability to control the collection, use, and dissemination of his or her PII. Mechanisms used include:

- Identifying uses and users of PII
- Seeking agreement to use PII
- Limiting PII collection
- Limiting use of PII to identified purposes
- Being open, honest, and respectful of individuals and their desire for privacy
- Providing avenues for complaints
- Allowing access to PII to maintain accuracy and completeness

The traditional view is that it is not possible to have good privacy without good security since security mechanisms, such as access controls, often protect privacy. However, it is increasingly being recognized that good privacy practices also encourage good security practices. For example, access to PII typically comes with legal requirements for need-to-know that call for more granular access controls to ensure that only authorized individuals have access to PII. This also helps to ensure that use of PII is limited to authorized purposes and has the added benefit of exposing the “need to know” discussion to other types of information that may also benefit from more granular access controls than would otherwise have been considered. Additional examples of how privacy and security work together are provided in the table below. Areas that privacy and security have in common include risk management; safeguards, access control, and encryption; data quality and integrity; retention and destruction; audit and accountability; and breach management. It is important for the security and privacy groups within an organization to work closely together in order to successfully address privacy risk.
Table 2. Examples of How Privacy and Security Work Together

<table>
<thead>
<tr>
<th>Common Areas</th>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>Conduct security risk assessments and determine how to address risks</td>
<td>Conduct privacy risk assessments (e.g. PIAs) and determine how to address risks</td>
</tr>
<tr>
<td>Safeguards, Access Control, &amp; Encryption</td>
<td>Implement security controls and protection mechanisms to control access to information</td>
<td>Implement safeguards to prevent unauthorized PII access and disclosures of PII</td>
</tr>
<tr>
<td>Data Quality &amp; Integrity</td>
<td>Protect the confidentiality, integrity, and availability of information</td>
<td>Ensure PII used to make decisions is accurate, timely, and complete</td>
</tr>
<tr>
<td>Retention &amp; Destruction</td>
<td>Ensure that data cannot be recovered once deleted</td>
<td>Delete PII once it has served its purpose and in accordance with approved retention schedules</td>
</tr>
<tr>
<td>Audit &amp; Accountability</td>
<td>Monitor and audit (e.g. continuous monitoring, periodic reviews)</td>
<td>Hold individuals accountable for protecting PII (e.g., audit and review)</td>
</tr>
<tr>
<td>Breach Management</td>
<td>Respond to security incidents</td>
<td>Respond to privacy incidents (e.g. security incidents involving PII)</td>
</tr>
</tbody>
</table>

Privacy Harms

Privacy is critical for an organization’s operations. If privacy is not adequately protected, there can be serious consequences both for the organization itself as well as for the individuals whose PII is collected and used. Consequences for the organization include large costs due to recovery efforts from privacy incidents, and loss of credibility, confidence, and trust in the organization from the public, partners, and other stakeholders. For individuals, consequences of inadequate privacy protection include negative impacts such as embarrassment or identity theft and other types of fraud. Daniel J. Solove has developed a taxonomy of privacy which illustrates the different harms that can occur. The taxonomy is presented in the table below. It provides information on harms in four types of areas: Information collection, information processing, information dissemination, and invasion. Harms that are listed that are frequently mentioned in discussions about privacy include surveillance and breach of confidentiality. However, Solove’s list also includes harms like aggregation, which is increasingly receiving attention as more and more data about individuals is aggregated into large databases, and intrusion, which is when acts occur that disturb an individual’s solitude or tranquility.

Table 3. Privacy Harms

<table>
<thead>
<tr>
<th>Type</th>
<th>Harm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Surveillance</td>
<td>Observation and/or capturing of an individual’s activities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Information Collection</strong></th>
<th><strong>Interrogation</strong></th>
<th>Actively questioning an individual or otherwise probing for information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Processing</strong></td>
<td><strong>Aggregation</strong></td>
<td>Combining multiple pieces of information about an individual to produce a whole that is greater than the sum of its parts</td>
</tr>
<tr>
<td></td>
<td><strong>Identification</strong></td>
<td>Linking information to specific individuals</td>
</tr>
<tr>
<td></td>
<td><strong>Insecurity</strong></td>
<td>Failure to properly protect individuals' information</td>
</tr>
<tr>
<td></td>
<td><strong>Secondary Use</strong></td>
<td>Using an individual's information without consent for purposes unrelated to the original reasons for which it was collected</td>
</tr>
<tr>
<td></td>
<td><strong>Exclusion</strong></td>
<td>Denying individuals knowledge of and/or participation in what is being done with their information</td>
</tr>
<tr>
<td><strong>Information Dissemination</strong></td>
<td><strong>Breach of Confidentiality</strong></td>
<td>Revealing an individual's information despite a promise not to do so</td>
</tr>
<tr>
<td></td>
<td><strong>Disclosure</strong></td>
<td>Revealing truthful information about an individual that negatively affects how they are viewed by others</td>
</tr>
<tr>
<td></td>
<td><strong>Distortion</strong></td>
<td>Spreading false information about an individual</td>
</tr>
<tr>
<td></td>
<td><strong>Exposure</strong></td>
<td>Revelation of things we normally conceal from most others</td>
</tr>
<tr>
<td></td>
<td><strong>Increased Accessibility</strong></td>
<td>Rendering an individual’s information much more easily obtainable</td>
</tr>
<tr>
<td></td>
<td><strong>Blackmail</strong></td>
<td>Threat to disclose an individual’s information against their will</td>
</tr>
<tr>
<td></td>
<td>** Appropriation**</td>
<td>Using someone’s identity for another person’s purposes</td>
</tr>
<tr>
<td><strong>Invasion</strong></td>
<td><strong>Intrusion</strong></td>
<td>Acts that disturb an individual’s solitude or tranquility</td>
</tr>
<tr>
<td></td>
<td><strong>Decisional Interference</strong></td>
<td>Others inserting themselves into an individual’s decision-making regarding their personal affairs</td>
</tr>
</tbody>
</table>

**Global Privacy Approaches**

Views of privacy around the globe vary. For example, privacy is seen as a right in the European Union, while in the U.S., attitudes about privacy are often influenced by market forces. The adoption of different privacy models represents varying views of privacy among countries which may be due to different historical, economic, and cultural influences on nations. The U.S. has a sectoral approach to privacy protection in that different economic sectors operate under different privacy laws. Privacy laws are enacted to respond to specific problems within sectors. Sectors that are not subject to specific privacy laws operate under self-regulation. For example, the Health Insurance Portability and Accountability Act (HIPAA) applies to the healthcare sector, specifically to healthcare providers, health plans, and healthcare clearinghouses and their business associates. In general, HIPAA requires patients to provide consent before their health information is shared with other organizations, with some exceptions. The Gramm-Leach Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, applies to
financial institutions. It requires financial institutions to securely store financial information, provide notice regarding how financial information is shared, and provide consumers with the option in some instances to choose to not share their personal financial information. In addition to sectoral laws, the Federal Trade Commission (FTC) can bring enforcement actions against “unfair and deceptive” trade practices by private sector organizations as authorized by the Federal Trade Commission Act, and many of these FTC enforcement actions have been given to organizations when they did not meet the commitments described in their privacy policies. In addition to federal privacy laws, states have enacted privacy laws as well.

In the U.S. public sector, there are two key privacy laws that apply to federal government organizations. The Privacy Act is based on the Fair Information Practice Principles, and controls the use of personal information by restricting federal agencies' collection, maintenance, use, and dissemination of personal information. It also requires agencies to allow individuals to access information about themselves that agencies maintain, and correct their records when the information is not accurate, relevant, timely, or complete. The E-Government Act requires federal government organizations to post privacy policies on agency websites used by the public and translate privacy policies into a standard machine-readable format. It also requires all agencies to conduct a Privacy Impact Assessment (PIA) before developing or procuring systems that collect, maintain, or disseminate information from or about members of the public. The Privacy Act contains limited exceptions to its general provisions for situations where providing individuals with access to their PII may harm agencies’ ability to conduct investigations of those individuals, e.g., in law enforcement and the intelligence community. The E-Government Act also contains some limited exceptions where PIAs are not required to be completed, e.g., for national security systems. Privacy in the federal government is overseen by the Office of Management and Budget, which issues guidance for federal organizations.

While some U.S. laws apply only to the private sector, and other laws, such as the Privacy Act and the E-Government Act, apply only to federal government organizations and contractors acting on their behalf, there are some laws that apply to organizations in both sectors depending upon the function that they perform. For example, the Children’s Online Privacy Protection Act (COPPA) applies to operators of websites and online services that are directed to children under the age of 13, regardless of whether the websites or services are operated by entities in private industry or the government.

In contrast to the U.S.’s sectoral approach to privacy, a comprehensive model features the use of comprehensive data protection laws regarding the collection, use, and sharing of PII, and the laws apply to both the private and public sectors. Enforcement is overseen by a designated official or agency. The European Union employs use of a comprehensive model, and the primary privacy law is the European Union Data Protection Directive. The Directive applies to all sectors and all types of personal data. In general, the Directive does not allow collection or use of personal data unless permitted by law. Other privacy models in use around the world include the self-regulatory model, where codes of practice for protecting PII are used, and the co-regulatory model, where a combination of law and self-regulation codes of conduct and behavior are used.
Privacy Engineering

There can be significant privacy impacts in the use of different technologies. In particular, newer technologies that have received attention for privacy impacts associated with their use include body scanners, social media, facial recognition, wearables, unmanned aircraft systems, cloud computing, connected vehicles, smart energy, and new forms of biometrics. Privacy risk for new technologies can be reduced significantly if privacy is addressed as systems are developed and implemented instead of waiting until they are almost operational before adding privacy protection. The concept of Privacy by Design (PhD)\(^6\) supports the idea that organizations should ensure that they protect privacy by default. This is accomplished not just through compliance with regulatory frameworks, but also by building privacy protection into business practices and physical design as well as policies. Privacy should be integrated into each layer of the organization; this comprehensive approach ensures that privacy risk is fully and proactively addressed.

Leveraging existing systems engineering processes and integrating privacy into them instead of creating separate processes to address privacy risk is a sound approach to use to implement Privacy by Design. The process of privacy engineering does this by integrating activities and associated methods that support privacy's unique features (e.g., notice, consent, PII collection limitation, individual access) throughout the systems engineering life cycle from the very beginning. The figure below shows the stages of the classic systems engineering life cycle and maps the core privacy engineering activities to the different life cycle phases. The privacy engineering activities can be mapped to any systems engineering life cycle regardless of type (e.g., agile, waterfall) since the core activities exist in every life cycle.

![Privacy Engineering Framework](image)

**Figure 1. Privacy Engineering Framework\(^7\)**


\(^7\) MITRE Corporation, Privacy Engineering, [http://www.mitre.org/privacy](http://www.mitre.org/privacy). For additional details on privacy engineering inputs, activities, and outputs for each life cycle activity in the figure above, refer to MITRE’s Privacy Engineering Framework at [www.mitre.org/privacy](http://www.mitre.org/privacy).
Key elements of privacy engineering include addressing privacy in design documentation, explicitly identifying technical privacy requirements for a system, constructing privacy tests based on those requirements, executing the privacy tests, identifying residual privacy risks, and determining how to address them. Privacy requirements must take into account architectural, technical, and policy controls, and address privacy risks beyond compliance. Many systems currently complete these life cycle activities with respect to security, but may not fully complete them regarding privacy, resulting in privacy risks not being adequately addressed. System documentation that should discuss privacy considerations includes design and requirements documents, test case specifications, test plan results, post-test results documents/risk register, and remediation plans. In addition, if a Privacy Impact Assessment (PIA) or other similar type of privacy risk analysis is completed, it should be updated at each milestone in the systems engineering process.

Privacy and Project Management

Project managers who oversee projects where PII is collected and/or used by technology should ensure that the different aspects of privacy discussed in the sections above are addressed in their projects, including using the Privacy Engineering Framework to ensure that privacy is addressed throughout the systems engineering life cycle. Regardless of the type of technology being developed or used, project managers should address privacy in the different project management areas as follows:

- **Scope management:** Include addressing privacy considerations in the overall project scope. In particular, ensure that technology-specific and environment-specific privacy requirements, including laws and guidance that apply, are reflected when identifying overall project requirements.

- **Project time and cost management:** Addressing privacy in projects may result in the need for additional activities that are not required in projects where PII is not collected and/or used, such as the creation of documentation that discusses privacy requirements, risks, and mitigations; use of privacy professionals to provide expert input on privacy issues; and extra quality control reviews to ensure that all privacy issues are addressed. These additional activities may result in more time and increased cost. Thus, the project manager should be sure to include these extra activities in the project schedule and budget so that enough project resources are acquired to adequately address privacy.

- **Project risk management:** Include privacy when identifying risks and planning risk responses, and document privacy risk in the risk register. Recognize that it may be difficult to conduct a quantitative risk analysis for privacy. Some estimates of costs related to breaches are available. For example, one study in 2014 found that data breaches cost companies an average of $201 per compromised record. However, extensive quantitative data regarding the cost of not adequately addressing all types of privacy incidents are not readily available for all environments.

---

- Project procurement management: Ensure that contracts contain clauses requiring vendors or service providers to meet privacy requirements. These clauses should include, when appropriate, requiring vendors or service providers to follow established procedures to report any privacy incidents that occur to designated authorities as well as the project manager.

- Project communications management and project stakeholder management: An organization's privacy program typically performs privacy activities in several main areas, including leadership, privacy risk management and compliance documentation, incident response, notice and redress, privacy training and awareness, and accountability. The privacy program ideally flows from the organization's formally defined mission, vision, goals, and strategy. Privacy program leaders and staff engage with both internal and external groups who are privacy stakeholders to inform them of the organization's privacy approach and collaborate with them regarding addressing privacy risk. The role of the privacy program in an organization is illustrated in Figure 2 below.

![Organizational Mission, Vision, Goals, and Strategy](image)

![Privacy Program](image)

**Figure 2. The Privacy Program's Role in an Organization**

In many cases, project managers who oversee projects where PII is collected and/or used by technology will be located in the information technology group or in program offices
or business divisions within an organization. Regardless of where he or she is located in the organization, the project manager should actively engage with the leaders of an organization's privacy program who are responsible for overseeing privacy risk management within an organization's different portfolios and programs. The project manager should work with privacy program leadership to ensure that the project addresses any specific privacy concerns expressed by the internal and external privacy stakeholder groups. In many cases, the project manager may also need to interact directly with some privacy stakeholders regarding privacy requirements. Among the privacy stakeholder groups, key privacy stakeholders whose expectations and needs the project manager should analyze and manage include:

- **External groups**
  - The public: Should be provided with notice regarding an organization's privacy practices, and, as appropriate, should be given the ability to consent to the collection and use of their PII, and the ability to review the PII held about them, correct it, and challenge compliance with stated privacy practices.
  - Information sharing partners: Could potentially have different views regarding privacy and/or the need to follow different privacy laws and guidance, which will need to be addressed when determining the project scope and requirements.
  - Vendors: Should provide privacy protection while performing services or providing products as stipulated in their contracts.

- **Internal groups**
  - Senior leadership: May make privacy risk decisions, especially regarding acceptable residual privacy risk, and set the standard for how privacy is addressed by the organization. How well an organization manages privacy risk ultimately flows from the top of the organization on down.
  - Information security: Responsible for identifying security mechanisms that protect privacy and for working closely with privacy in order to address privacy risk.
  - Human resources: Responsible for protecting PII of employees and applicants.
  - Legal counsel: Responsible for interpreting privacy laws and guidance so that they are applied appropriately within an organization's environment.
  - Procurement: Ensure that privacy requirements are included in contracts.
  - Records management: Responsible for identifying and documenting records retention schedules. One of the best ways to reduce privacy risk is to not retain PII longer than it is needed.
  - Communications/public affairs: Assist with providing notice to the public regarding the organization's privacy practices and also with engaging with other external privacy stakeholders.
Key privacy stakeholders should be listed in the project’s stakeholder register and interaction with them should be addressed in the project communications management plan and stakeholder management plan as appropriate.

Conclusion

Privacy concerns continue to grow as the number of new technologies that collect, use, and/or share PII increases and as existing technologies are used in new ways. By using privacy engineering and incorporating the topic of privacy into the processes used in the different project management areas, project managers can ensure that privacy risk is adequately addressed in the use of technology.

References