Privacy Engineering & Assurance

The Emerging Engineering Discipline for implementing Privacy by Design

Contents

Privacy Engineering & Assurance

The Emerging Engineering Discipline for Implementing Privacy by Design

1 Introduction

Privacy related risks are becoming more and more present in our everyday life as more and more data is being automatically created and as our life has taken on a digital shape. In addition, analytical tools have become very powerful and enable unprecedented understanding of individual actions and behaviour. Data is the new asset class[1] and has become the power that moves the machinery of the internet and web. The data centric business models have proven to be very successful resulting into more and more incentives to collect and process personal data[2].

This has raised concerns[3] from consumer advocates, parliamentarians and data protection supervisors that consumers need products that take into account the principles of Privacy by Design (PbD)[4]. The privacy principles and concepts of PbD are valid, but they do not answer the question of "How do you do it, in practice?" There is an increasing emergence of legislative work around privacy, but that will not answer the "How?", either. At the same time, today, privacy is implemented in this technology dominated world. It is the engineers of these technologies who need the answer to "How?" Today we lack methodologies and we lack the technology professionals who "grok"[5] privacy.

Privacy Engineering and Assurance is the engineering methodology to bridge the gap between laws and principles and technologies and is intended to foster the birth of the new professional "Privacy Engineer".

[1] World Economic Forum,"Personal Data-New Asset-Report", January 2011, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

[2] Billy Ehrenberg, The Guardian, "How much is your personal data worth?", April 2014, http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth.

[3] US Federal Trade Commissions, "Protection Consumer Privacy in an Era of Rapid Change", Executive Summary, December 2010, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

[4] Dr. Ann Cavoukian, "7 Foundational Principles of PbD", http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/.

[5] Oxford Dictionary, Understand (something) intuitively or by empathy, http://www.oxforddictionaries.com/definition/english/grok.

The solution is the development of a software engineering discipline to take Privacy by Design from a subjective set of seven essential principles into a framework for implementation of privacy in the product creation process. The objective of this discipline is Privacy Engineering and its complementary discipline of Privacy Assurance; compositely called Privacy Engineering & Assurance.

2 The Discipline

The Privacy Engineering & Assurance discipline provides a systematic and engineering compatible approach to implement Privacy by Design, rather than an ad hoc approach of checklists of “dos and dont’s”. This discipline serves as an industry best practice and is an essential element for accountable organizations that recognize the need for strong business practices.

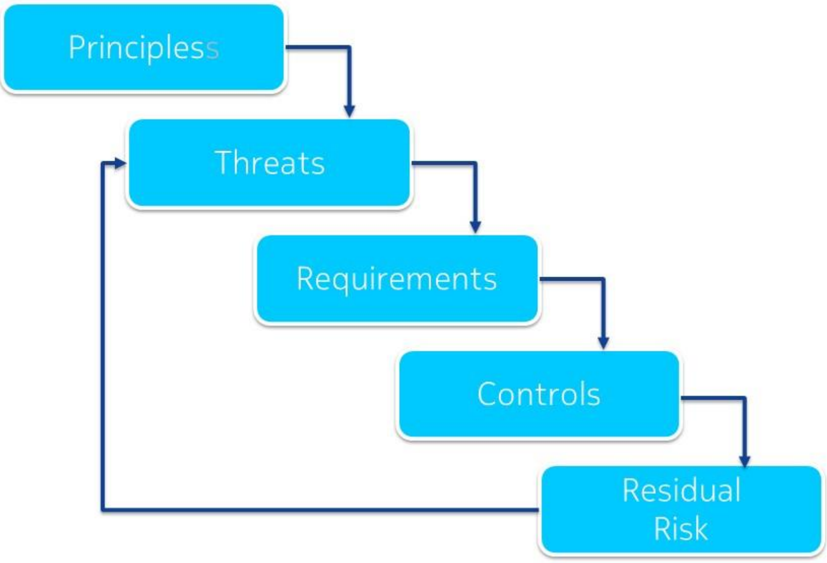
As a discipline, Privacy Engineering & Assurance needs to:

1. Consist of two components: i) Privacy Engineering ,which identifies privacy threats and risks, as well as designs and implements privacy safeguarding controls into products and services; and ii) Privacy Assurance, which verifies the products and services conformance to such privacy safeguarding controls and regulatory compliance;
2. Be based on an industry accepted privacy knowledge base consisting of privacy principles[6], privacy related threats and their underlying engineering vulnerabilities, privacy risks that could harm individuals[7], privacy safeguarding requirements and guidelines and design patterns for implementing privacy safeguarding controls.
3. Ensure compliance with applicable data protection and other privacy laws;
4. Be based on and compatible with best industry guidance for software engineering as defined by the IEEE Software Engineering Book of Knowledge[8];
5. Integrate a code of ethics and professionalism into the discipline, based on ACM Software Engineering Code of Ethics & Professional Practice[9];
6. Leverage existing disciplines of product security and business continuity and their associated processes, activities and tools;
7. Be an integral mechanism for managing privacy risks in a broader organizational risk management context;

[6] For example, The 11 privacy principles of ISO 29100 – Privacy Framework, http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip.
[7] Centre for Information and Policy Leadership, “A Risk-based Approach to Privacy: Improving Effectiveness in Practice”, June 2014, http://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf.
[8] IEEE Computer Society, “Guide to the Software Engineering Book of Knowledge (SWEBOK)”, Version 3.0, http://www.computer.org/portal/web/swebok/swebokv3.
[9] ACM, “Software Engineering Code of Ethics and Professional Practice”, Version 5.2, http://www.acm.org/about/se-code.

8. Create demonstrable evidence that accountable organizations are utilizing best practice processes in identifying, analyzing and mitigating privacy risks.

Following diagram illustrates the interplay between the essential elements of a privacy knowledgebase:



Implementing Privacy by Design

Application of the discipline involves using threat analysis and mitigation methodologies, as well as risk assessment and mitigation methods. Additionally, implementation and testing in the product creation process necessitates development of best practices for coding and testing for privacy, based on the application of similar guidance from the product security discipline. In fact, the inter-dependent nature of privacy and security means that other methods needed in Privacy Engineering & Assurance can be based on the analogous methods used today by Product Security Engineering.

As a discipline of software engineering, there needs to be professional societies and educational institutions committed to educating software engineers in the essential knowledge and skills, as well as providing for professional certification and diploma based degree program. There is already some initial evidence of such programs[10] [11] [12].

[10] IAPP, CIPT Certification Program, https://privacyassociation.org/certify/cipt/.
[11] NIST, " NIST, IAPP Host Privacy Engineering Workshop", August 2014, http://www.nist.gov/itl/privacy-081214.cfm.
[12] Carnegie Mellon University, MSIT-Privacy Engineering Degree Program, http://privacy.cs.cmu.edu/.

3 The Process

The Privacy Engineering & Assurance Process (PEAP) is a set of proactive engineering activities to identify the privacy impact of a given object, to design controls and mitigations to ensure appropriate Privacy by Design, and then verify that the implementation is complete and operational, while documenting evidence of this state for reference of regulatory compliance and in the event of a privacy breach. This means building privacy into the object as part of its complete product creation lifecycle. The object can be a software or a hardware product, service, process, operation or even a contract or a partnership.

The PEAP, when leveraged together, takes Privacy by Design from a set of principles to a product reality. The objectives of the PEAP include:

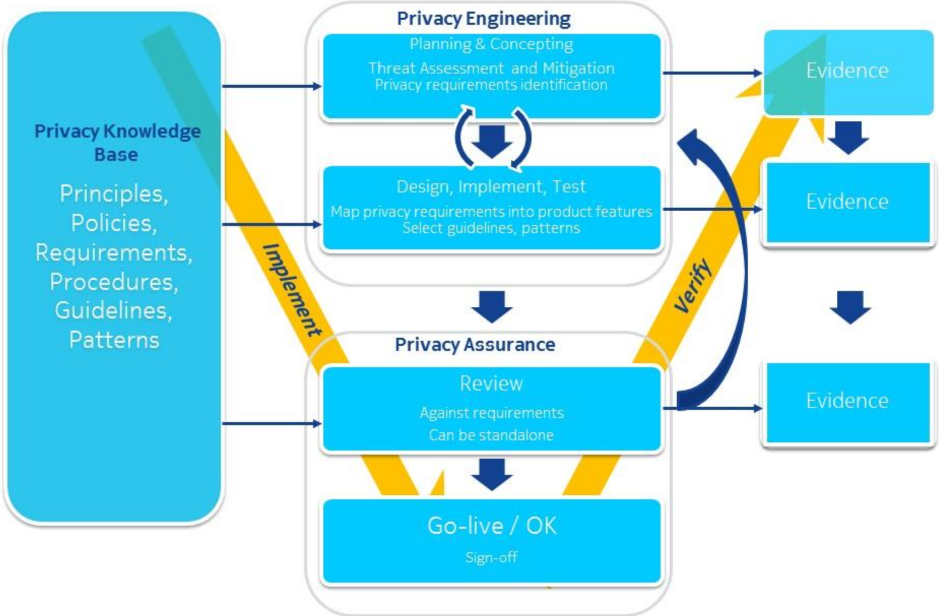
- Identify and assess privacy risks and propose mitigations;
- Include a review decision point as a mandatory condition for product release;
- Conform to industry best practices for process definition;
- Defined and documented such that it is repeatable for even a privacy "newbie";
- Deployable as Standard Operating Procedure within businesses, independent of the particular Product Creation Process[13] used by the organization;
- Create compliance evidence with storage integrity and availability on-demand;
- Based on accepted knowledge base of privacy principles, threats, risks, requirements, guidelines and patterns;
- Leverage industry standards, applicable industry best practices;
- Equally applicable for use in self-assessment or third-party-assessment;
- Openly available within the organization;
- Used both for communication and training purposes;
- Externally accepted evidence of an accountable, privacy compliance business process;
- Stable, stands the test of time, organization changes do not require process changes;
- Useful evidence in third-party contracts of the best practice for implementing Privacy by Design.

The Privacy Engineering component of PEAP consists of an iteration of a threat identification and mitigation cycle to ensure that privacy is appropriately considered and privacy requirements are included in the object, from the beginning to end of its product creation lifecycle, not as an afterthought.

[13] For example waterfall, prototyping, iterative and incremental development, spiral development, rapid application development, and extreme programming.

The Privacy Assurance component of PEAP consists of assessment to verify that identified privacy requirements have been implemented into control points within the object and are functioning appropriately. In addition, a mandatory review is required, prior to release of the object. This "Go-Live" review verifies whether there is satisfactory evidence that steps have been taken in implementing privacy into the object. The review is conducted by roles with responsibility for the Privacy Engineering of the object (E.G., Privacy officer, Privacy champion, Program management, Development team).

Visually, the PEAP elements are to be viewed as divided between the knowledge base of privacy, those associated with implementation, Privacy Engineering, those associated with verification that requirements have been implemented and are operational, Privacy Assurance.


Privacy Knowledge Base
Principles, Policies, Requirements, Procedures, Guidelines, Patterns
Privacy Engineering
Planning & Concepting
Threat Assessment and Mitigation
Privacy requirements identification
Design, Implement, Test
Map privacy requirements into product features
Select guidelines, patterns
Implement
Verify
Privacy Assurance
Review
Against requirements
Can be standalone
Go-live / OK
Sign-off
Evidence
Evidence
Evidence

Elements of the Privacy Engineering & Assurance Process

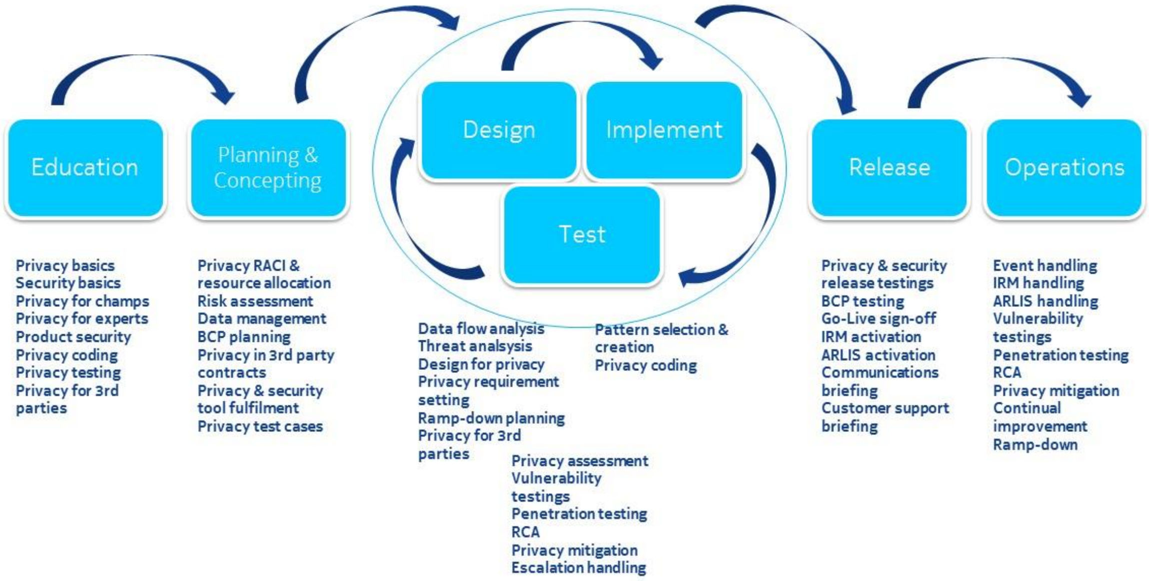
Underlying PEAP is the notion that privacy is to be considered throughout the product lifecycle. Privacy related activities become an integral part of Education, Planning & Concepting, Design, Implementation, Testing, Release and Operational phases of the product lifecycle.

Clear identification and sourcing for roles and responsibilities for each privacy stakeholder is essential to executing PEAP in an efficient and productive manner. Use of role/responsibilities assignment models such as the RACI model are effective approaches to ensure clarity[14]. A basic set of roles includes that of Legal counsel, Privacy officer, Privacy champ, Program manager, Product

[14] Wikipedia, "Roles assignment matrix", http://en.wikipedia.org/wiki/Responsibility_assignment_matrix.

manager, Development manager, QA or Test manager, and External communications manager. The individuals supporting these roles represent the extended Privacy Team for the product.

Out of necessity, the PEAP process needs to be defined at a high level, such that it can be adopted by different organizations with different businesses. The process also needs to be sufficiently flexible to be adaptable to different product creation process styles. And the process needs to be malleable to context, whether the object being created is software or a hardware product, service, process, operation or even a contract or a partnership. While malleable to context, it is also important that if the current context has negligible privacy impact, then the particular process step should be omitted, such as if the release has no material change from previous releases, then no sign-off review would be needed.



Mapping privacy activities on to product creation process

There has been significant amount of research on the use and methodology for a Privacy Impact Assessment[15]. As noted by the UK ICO PIA Handbook, notes, it is "difficult to write a 'one size fits all'" guidance on how to conduct a privacy assessment[16]. Products with a two week release cycle, such as a web application need an appropriately terse approach. Complex financial systems, that may have

[15] UK ICO and Trilateral Research & Consulting, "Privacy impact assessment and risk management", May 2013, http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Corporate/Research_and_reports/trilateral-full-report.pdf.

[16] UK ICO, "Privacy Impact Assessment Handbook", Version 2, http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

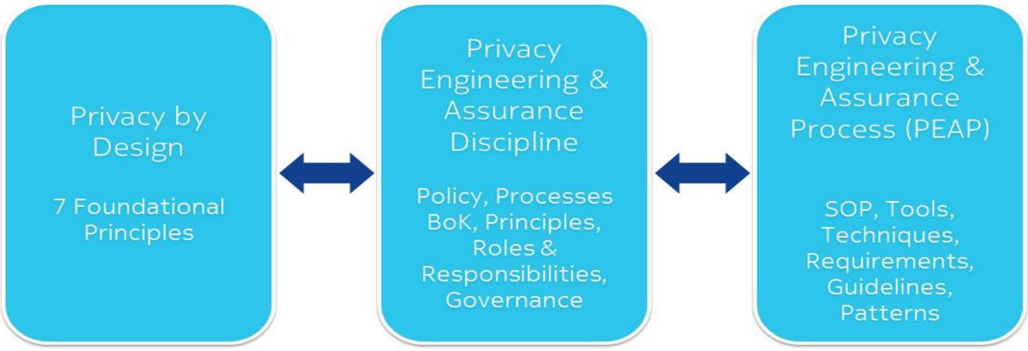
multi-year release cycles, necessitate a more rigorous assessment, appropriate for regulated industries. No matter the depth of methodology, the goal remains to provide a tool that you can use to identify and reduce the privacy risks in a product. The privacy assessment is an integral activity to PEAP. These assessments can be either self-assessments or conducted by a 3rd-party. Ultimately, evidence is essential documentation of the context and provides assurance that privacy requirements have been implemented into the product.

The PEAP creates an important link between privacy risks and product requirements that is intended to safeguard privacy. It also creates a link between privacy controls and evidence that the controls have been implemented and are functioning appropriately.

4 Conclusion

The adoption of a Privacy Engineering & Assurance discipline is a necessity in the era of the internet and web. The discipline transposes Privacy by Design into a business management system. The discipline is based on best industry guidance for software engineering. It also needs to integrate a code of ethics and professional practice, also borrowed from best industry guidance. The discipline needs to be supported by professional certification and educational academic curriculums that provide a source for needed software engineering resources.

The Privacy Engineering & Assurance Process provides the mapping on to software engineering best practices. Tools and techniques are needed to provide a Privacy Engineer a toolkit to support engineering and assurance needs. Many of the tools, activities and techniques can be created, based on those existing in the product security discipline, but adapted for privacy.



Privacy by Design

7 Foundational Principles

Privacy Engineering & Assurance Discipline

Policy, Processes BoK, Principles, Roles & Responsibilities, Governance

Privacy Engineering & Assurance Process (PEAP)

SOP, Tools, Techniques, Requirements, Guidelines, Patterns

Transposing PbD to PEAP

Best practices for privacy requirements, guidelines, and patterns will need to be catalogued for common use by Privacy Engineers across organizations. Those who doubt the practicality of Privacy by Design need to look no further than the emerging discipline of Privacy Engineering & Assurance.