MITRE's Privacy Engineering Tools and Their Use in a Privacy Assessment Framework

10 October 2019

Julie McEwen, Privacy Engineering Capability Area Lead, MITRE Corporation, jmcewen@mitre.org

Stuart Shapiro, Principal Cyber Security & Privacy Engineer, MITRE Corporation, sshapiro@mitre.org

Organizations collect and use personally identifiable information (PII) about individuals for many uses, including to provide services and benefits. Many organizations have not fully integrated privacy into their systems engineering processes. Privacy engineering, a systematic, risk-driven process, helps ensure that privacy is addressed from the very beginning as systems are developed.

Organizations face severe consequences for not protecting privacy. Some of the scenarios include: reduced organizational effectiveness; curtailment of some programs; a negative impact on people whose PII has been collected, including identity theft; large costs for recovery from privacy incidents; and loss of credibility, confidence, and trust in the organization from affected individuals, the public, and stakeholders.

Privacy engineering focuses on methods and standards, technical elements of information infrastructure, and individuals and collectors. Members of MITRE's Privacy Engineering Capability review organizations' capabilities and identify how they can integrate privacy into systems engineering processes and documentation.

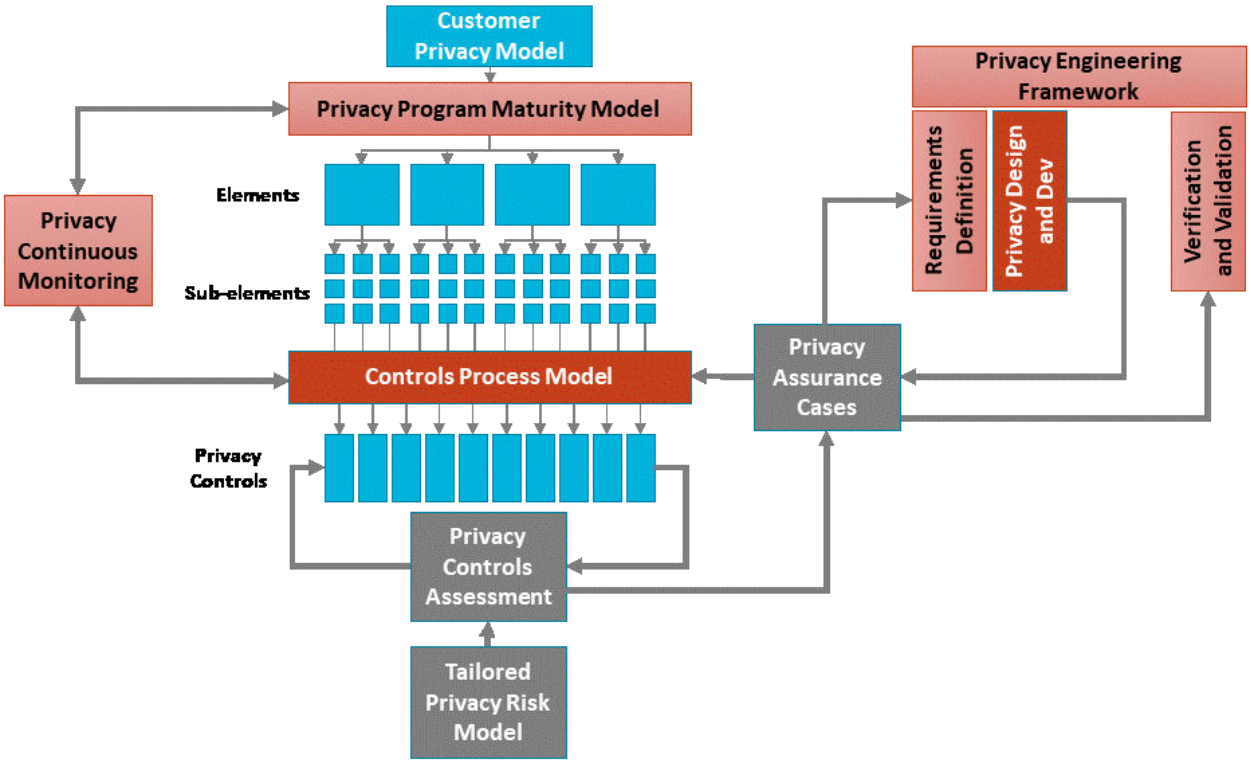
MITRE has been working for over two decades to develop multiple resources that weave privacy risk management into the enterprise and its systems. MITRE's Privacy Engineering Capability has created a suite of privacy engineering tools for use by privacy professionals in their privacy engineering work to help organizations advance the state of privacy. The tools are described in the table below.

Summary of MITRE Privacy Engineering Tools

Tool	Description
Privacy Engineering Framework and Lifecycle Adaptation Guide	Framework that can be used to integrate privacy into the traditional systems engineering "V" life cycle. Guidance for adapting the Framework to other life cycles beyond Waterfall types, such as Agile (incremental) and Spiral (iterative) life cycles, is provided in an Appendix.
Privacy Maturity Model	Framework for developing, implementing, maintaining, and evaluating privacy programs. Privacy programs must be comprehensive enough to address all requirements established by authoritative sources (e.g., laws, regulations, guidance), and must be supported by written policies, appropriate training, ongoing practices, and appropriate assessment. This model may be used to assess both *completeness* (whether an organization has identified and implemented all elements of a privacy program) and *maturity level* (an evaluation of to what degree practices supporting each element are effective in achieving their intended purpose). It was developed based not only on comprehensive research of relevant laws and guidance, but on practices that have been assessed as effective in many organizations.

Generic System Privacy Requirements and Tests	Set of generic privacy requirements and tests that can be used to verify that a system works as expected from a privacy perspective.
Privacy Continuous Monitoring Framework	OMB Circular A-130, *Managing Information as a Strategic Resource*, requires every US federal government agency to conduct privacy continuous monitoring and to have a privacy continuous monitoring program and strategy. This document identifies privacy-specific activities to adopt to implement privacy continuous monitoring.

The MITRE privacy engineering tools can be used individually or together. The light red boxes in the diagram below illustrate where MITRE privacy engineering tools can be used in an overall Privacy Assessment Framework.



The Role of MITRE Privacy Engineering Tools in a Privacy Assessment Framework

MITRE's Privacy Engineering tools are available at www.mitre.org/privacy. For questions or comments on the tools or assistance with their use, contact privacy@mitre.org.