Privacy Engineering…It's Time to Take the Next Steps towards Standards and Automated Tools

By Gail Magnuson
President
Gail Magnuson, LLC
Gail.Magnuson@gmail.com
704-232-5648

For years, privacy professionals have worked towards transitioning the implementation of data protection from an art to a science, especially when working with IT developers.

Over the past quarter century, the privacy profession has made slow but steady progress towards the development of a more rigorous privacy engineering discipline that results in comprehensive privacy by design implementations. We are now beginning to see results.

This engineering journey can best be summarized as creating the linkages from principles and regulations; to policies; set in the context of a rigorous privacy analysis; translated into privacy controls; defined in services/functions; implemented in technical and procedural mechanisms and; reported using tools that allow a privacy engineer to demonstrate compliance.

Up until recently, the privacy office has been challenged to translate regulations and high-level principles into guidance for the IT professional. Often this guidance includes recommendations that exceed the product or system design criteria itself.

This is no easy task in a world where every dimension of the environment is changing rapidly. For example, businesses are more global; principles are expanding; global regulation and data protection authority orders are changing; IT development techniques are more agile; technology is exploding and; structured and unstructured data is everywhere.

It becomes almost impossible for a privacy engineer to work side by side with IT without a repository that provides the privacy engineer with a library of previously developed privacy solutions that can be pulled off the shelf and reused and modified for the next use case or user story.

Up until now such privacy repositories, if they exist at all, belong to the large global and consulting companies. These companies have large privacy offices or a fleet of

consultants that have performed many analyses over many years. While they may/may not have integrated privacy repositories, they have designed agile techniques and have employed tools that make their jobs easier for their clients.

They may also have individuals on staff that fulfill the job of a privacy engineer. While they may not be called privacy engineers they bridge the gap between privacy and technology.

It's past time for more privacy offices to address the privacy engineering challenge. When a data protection authority comes knocking, it will be important to be able to demonstrate that technical and procedural mechanisms are in place and working to implement the mandated privacy controls which in turn satisfy policies, regulations and principles.

More recently think tanks, standards development organizations, and privacy professionals and educators have studied and written about privacy engineering and privacy by design from many different perspectives. Privacy by design in short means that each new service or business process that makes use of personal data must take the protection of such data into consideration. An organisation needs to be able to show that they have adequate security and privacy in place and that compliance is monitored. In practice this means that an IT department must take privacy into account during the whole life cycle of the system or process development.[1]

For this discussion, the definition of privacy engineering is from The MITRE Corporation (MITRE).: "Privacy Engineering is a systemic, risk-driven process that operationalizes the privacy by design (PbD) framework within IT systems"[2]. The privacy engineer or a designated individual is the individual that performs privacy engineering.

Companies have/are building tools that automate parts of the engineering and accountability processes. The time is ripe to identify the work underway - who is doing/has done what - to help the privacy office understand how new developments in privacy engineering and privacy by design can help deliver accountable privacy.

This paper provides an overview of the progress the privacy engineering professionals have made from several different perspectives and cites examples of who has/is doing what. It focuses on how privacy legislation, principles and policies may be supported by privacy engineering standards; privacy engineering frameworks; privacy engineering models and methodologies; automated privacy engineering tools; risk management methodologies; libraries of privacy controls; books written recently about privacy

---

[1] http://www.eudataprotectionregulation.com/data-protection-design-by-default

[2] https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive-enterprises/privacy-systems-engineering

engineering; educational opportunities in privacy engineering; conferences devoted to privacy engineering; et.al.

It is by no means a comprehensive inventory, however it does demonstrate how far the privacy engineering discipline has progressed.

Privacy offices have always been challenged with the complexity of privacy legislation, principles and policies and the difficulty of translating that complexity to an IT systems engineer with precision without interfering with the creative product development processes and doing so with a limited privacy office budget. There are now several privacy offices that have done so successfully and protected their brands as trustworthy.

During the research for this paper there have been significant advances to transitioning privacy from an art to a science by following the privacy engineering trail. It is an exciting time for privacy and privacy engineering. The choices for the privacy office are now many and are summarized in the categories below.

- **Privacy Legislation, Data Protection Authorities and Industry Guidance;** For years, the privacy profession has been challenged to understand the various legal requirements from legislation and interpreted requirements from data protection authorities and industry associations. There are online resources are now available to assist the privacy office in defining the changing requirements for its organization. Nymity has a series of products that inform the privacy office of legislations, data protection authority and court findings and recommendations.

- **General Operational Privacy Management:** Overall guidance for how a privacy office might operationalize privacy and to attest to its implementation is available from several sources Nymity[3], for example has created a series of products that assists organizations in building a privacy office and attesting compliance. These significant contributions are precursor to transitioning to a privacy office that has a functioning privacy engineering discipline.

- **Privacy Engineering Models/Methodologies** are emerging. Some are comprehensive and others focus on a subset of the overall privacy engineering processes. Some are integrated into an overall IT engineering process and others are standalone. Some address the full life cycle of privacy implementation from engineering to implementation to accountability to remediation.

  The OASIS Privacy Management Reference Model and Methodology (PMRM)[4] provides a comprehensive approach to privacy engineering. The PRIPARE[5]

[3] www.Nymity.com
[4] http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html

((Preparing Industry to Privacy-by-design by supporting its Application Research) Privacy- and Security-by-Design Methodology Handbook made use of the PMRM as a foundation and defines the privacy engineering methodology at a more detailed level after researching the privacy engineering landscape. PRIPARE integrates its methodology into the various IT development processes.

- **Privacy Engineering Publications** have given privacy professionals significant privacy engineering direction and education. The following two books and public patent are among those: The Privacy Engineer's Manifesto Getting from Policy to Code to QA to Value[6], Privacy Engineering, Achieving Digital Trust The new rules for businesses at the speed of light[7], and Jeffrey Ritter's public patent US 7240213 B1 System trustworthiness tool and methodology[8]. Needless to say there are now far more publications and academic papers that focus on a comprehensive approach to privacy engineering and many more that address components of the privacy engineering life cycle.

- **Risk Management Privacy Engineering Methodologies:** Most privacy offices and their consultants take a risk-based approach to privacy compliance and engineering due to the complexities of the laws and the extensive personal information that is necessary to drive the organization. The Lunddun: a privacy threat analysis framework, the NISTIR 8062 Introduction to Privacy Engineering and Risk Management[9], and MITRE's Privacy Engineering Framework[10] have focused on risk management in the context of privacy engineering.

- **Privacy Engineering Automated Tools:** There are automated tools being developed that support the Privacy Engineering Models/Methodologies from the top down or at the Use Case or User Story level. For years privacy professionals have used matrices or visualization tools to demonstrate the flows of personal information. This has been a labor of "love" to develop, document and maintain.

  We are now being introduced to additional software tools that help us document data flows and keep them updated and even integrate the flows with certain

---

[5] http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

[6] https://www.amazon.com/Privacy-Engineers-Manifesto-Getting-Policy/dp/1430263555/ref=sr_1_1?ie=UTF8&qid=1488387856&sr=8-1&keywords=michelle+dennedy

[7] https://www.amazon.com/Privacy-Engineers-Manifesto-Getting-Policy/dp/1430263555/ref=sr_1_1?ie=UTF8&qid=1485540649&sr=8-1&keywords=privacy+engineering+manifesto

[8] https://www.google.com/patents/US7240213

[9] http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[10] https://www.mitre.org/sites/default/files/publications/14-2545-presentation-privacy-engineering-framework-july2014.pdf

privacy analyses. Nymity's Nymity SmartPIA[11] and OneTrust[12] are examples. Such tools often help automate privacy impact assessments and risk management analyses and integrate new visualization tools that assist the privacy office in presenting its analysis, findings and recommendations to a wide set of stakeholders and regulators.

Prifender[13] has developed a suite of tools that takes the next step. Prifender knows where "a company's" personal data flows, for example from jurisdiction to jurisdiction. et al. Naturally this requires an investment in documenting the privacy engineering information in terms of what information can be collected from whom/where, stored where, used for what in concert with the individuals' permissions, shared with whom, transferred where, and retained or destroy when. The benefit on the back end is to be able track the actual data flows and identify those that require remediation.

- **Official Standards:** Formal standards to support the Privacy Engineering Frameworks/Models/Methodologies are in process. Existing research specific to privacy engineering models/methodologies include the OASIS PMRM[14]. The OASIS PMRM is currently developing an open source tool that will automate the normative sections of the PMRM to demonstrate its viability as a standard. ISO/IEC JTC 1/SC 27 WG 5 has a future project to develop a Privacy Engineering Framework. While there are several standards that have been developed for privacy, there are few that that relate specifically to privacy engineering.

- **Privacy Controls, Design Strategies, and Patterns Libraries and Articles:** The privacy industry has focused on defining privacy controls, mixed in with policies and guidelines that can be adopted by privacy offices to instruct those in IT to implement. The NIST Special Publication 800-53, Appendix J[15] has long been a source of privacy controls. It is in the process of being upgraded. The Annex B of PRIPARE[16] also includes a list of Privacy Principles, Guidelines and Criteria for Requirements Operationalization. There are many more sources of privacy control statements from AICPA/CICA, APEC and other consultancies that are widely available. These libraries have been helpful to privacy offices in creating corporate specific privacy controls.

---

[11] https://www.nymity.com/products/smartpia.aspx

[12] https://onetrust.com/

[13] http://www.prifender.com/

[14] http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html

[15] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[16] http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

Design Strategies and Patterns have been developed to help translate a subset of privacy controls into functional designs and specifications for implementation. Examples of design strategies and patterns articles and websites include Privacy and Data Protection by Design – from policy to engineering[17] and UC Berkeley - School of Information's privacypatterns.org[18]

- **Privacy Principles and Data Protection Principles:** As various privacy offices embark to implement privacy engineering methodologies and tools it is important revisit the guiding principles and perhaps to create privacy by design principles and operating principles and update internal policies. Certainly, it is important to review self-regulating principles and standards from the industry organizations the corporation belongs to. It is also important to understand the emerging issues that new technology brings. Examples of recently updated privacy principles and comparisons are found in the PMRM[19] and the ISACA Privacy Principles and Program Management Guide[20]. The ISACA publication also "explains how enterprises can structure privacy initiatives to address privacy requirements and the aspects of a privacy governance and management program within the comprehensive COBIT 5 framework".

- **Privacy Engineering Education:** In 2015 Carnegie Mellon University graduated the first class of its Master of Science in Information Technology—Privacy Engineering[21] thanks to the leadership of Lorrie Cranor and her colleagues. Johns Hopkins University offers an online privacy engineering course[22] taught by Jeffrey Ritter. Other universities are not only offering privacy engineering courses, but are funding innovative privacy engineering research for their Masters and PhD candidates.

- **Privacy Engineering Conferences and Workshops:** IAPP has offered half-day workshops and presentations at its conferences for some time now on privacy engineering. IEEE is about to convene its third conference on May 25th in San Jose, the 2017 International Workshop on Privacy Engineering IWPE'17[23]. The 2016 International Workshop on Privacy Engineering IWPE'16 program materials[24] and their 2015 program materials[25] describe the various advances in

---

[17] https://arxiv.org/pdf/1501.03726v2.pdf

[18] https://privacypatterns.org/

[19] http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html

[20] https://www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/RESEARCHDELIVERABLES/Pages/ISACA-Privacy-Principles-and-Program-Management-Guide.aspx

[21] http://privacy.cs.cmu.edu/

[22] https://apps.ep.jhu.edu/course-homepages/3505-635.472-privacy-engineering-ritter

[23] http://ieee-security.org/TC/SPW2017/IWPE/

[24] http://ieee-security.org/TC/SPW2016/IWPE/program.html

[25] http://ieee-security.org/TC/SPW2015/IWPE/program.html

privacy engineering. These and other similar conferences are focused specifically on advances in privacy engineering research, advances and tools.

Privacy professionals have always focused on methodologies and processes that help bring the best value to the corporations they serve at the lowest expense possible. In doing so most privacy professionals have always gravitated to a top down analysis where they were able to replicate guidance from one design initiative to another. With the privacy engineering methodologies and supporting tools the privacy engineer will be able to work at a more granular level and ensure a more comprehensive and complete implementation of privacy mechanisms and demonstration of compliance.

As each privacy office focuses on the challenges of privacy engineering and the demonstration of accountability, it will be key to lay out a privacy engineering implementation plan that considers the key methodologies and tools that create the linkages from principles and regulations; to policies; set in the context of a rigorous privacy analysis; translated into privacy controls; defined in services/functions; implemented in technical and procedural mechanisms and; reported using tools that allow a privacy engineer to demonstrate compliance and execute remediation. This can be done.

For additional research in privacy engineering published in 2015 by PRIPARE has written Contribution to Study Period on Privacy Engineering Framework[26].

---

[26] http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D1.3_v1.0.pdf