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 and towards the development of a more rigorous privacy engineering discipline resulting in comprehensive privacy by design implementations.

This engineering journey can best be summarized as creating the linkages from principles and regulations; to policies; translated into privacy controls; defined in services; implemented in technical and procedural mechanisms; reverse engineered to demonstrate accountability.

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; and technology is exploding.

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

Up until now such libraries, 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 libraries, they have designed agile techniques and have employed tools that make their jobs easier.

They 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 the technical and procedural mechanisms have implemented the services which meet the mandated privacy controls which in turn satisfy the policies, regulations and principles.

More recently think tanks, standards groups and privacy professionals and educators have studied and written about privacy engineering and privacy by design from many different perspectives. Other companies have/are building automated tools that automate parts of the engineering process. It is time reflect on who is doing/has done what to help privacy offices make sense of privacy engineering and privacy by design so that more privacy offices may plan their journey.

To accomplish this task the following terms will be defined, the various contributions that relate to privacy engineering and privacy by design identified and then mapped to the categories to which they contribute. This exercise is intended to help frame the dialogue. The terms related to privacy engineering and privacy by design:

* Privacy Engineering
* Privacy by Design
* Principles
* Regulations & Orders
* Standards
* Frameworks
* Models
* Methodologies
* Controls
* Services
* Mechanisms
* Techniques
* Tools
* Privacy Engineering Courses and/or Degrees
* Risk Management
* Attestations
* Accountability

The providers include:

* tbd

The mapping is:

* tbd

The finding or observations are:

* tbd