

Privacy by 3PT[®]: A Management Model

Richard Purcell¹
Corporate Privacy Group
Nordland, Washington
USA

Privacy by 3PT[®] is a comprehensive management tool promoting privacy in a purposeful way. The model includes three major communities, four high-level dimensions and five supporting implementation methods. Over the last several years we have seen the emergence of good privacy practices being actively engaged by organizations for specific objectives and outcomes. Current pressures from markets, governments, and advocacy groups for privacy controls require active, positive responses from responsible organizations. ***Privacy by 3PT[®]*** provides a realistic, sustainable model for these organizations to develop, implement, monitor and measure data protection and consumer privacy programs that yield long-term value in risk management and customer trust.

Over the course of the last decade, data protection and consumer privacy have been the subject of both discourse and discord both within and between the USA and Europe. We have established some points of agreement and have agreed to disagree (for now) on others. These disagreements have tended to be begrudging rather than forgiving. Each side seems to believe that, given time, the other side will eventually see the error of their ways. In other words, we continue to fail to communicate with one

¹ Richard Purcell is CEO of Corporate Privacy Group, an independent privacy consulting practice dedicated to supporting the development of sustainable privacy programs. Formerly the Chief Privacy Officer at Microsoft, Mr. Purcell serves on the Boards of TRUSTe and the Int'l Association of Privacy Professionals. He lives and works in the Pacific Northwestern United States.

another. We can't seem to address the essentials of our positions; we can't understand why the other side 'just doesn't get it.'

We believe there is more to this lack of alignment than just stubbornness and historical context. One very basic disagreement concerns accountability for the rules of fair play. Both inside and between our regions, we haven't been able to achieve a common foundation for privacy. Yes, many Americans are reluctant to encourage broad government oversight; and certainly many Europeans can't see global corporations as compassionate guardians of public interests. But these dogmatic views are overly simplistic, unhelpful, and do little to help us understand one another. There is much more at play here than these rigid positions expose. There is a real failure underlying the disagreement; and poking each other with barbs grown dull from decades of use is an unlikely way to tease out a solution. This article does not attempt to produce the solution; we simply recommend a starting place using a management model designed to help us all succeed. If this model provides a newer, sharper stick with which to poke one another, then perhaps it will have served its purpose in seeking a global basis for privacy programs.

We contend that the lack of common agreement in data protection and privacy is quite understandable - it is due to the lack of widely recognized management models specific to this area. Over the last decade, concerns about technology security have stimulated the production of security models that have subsequently been implemented

in major corporate infrastructures². For the most part, these models have put to rest the disputes over technology security practices; indeed, they have proved the catalyst for moving from concept to action. As a result, we have stopped arguing over the need for security and begun implementing the practices needed to produce a more secure technical environment. Although we have not yet achieved that goal, we are at least on a common path toward it.

In the same way, we recognize that we have an important opportunity for developing a professional practice for privacy. Organizations have accepted the value, laws have set expectations and requirements (more comprehensively in some regions than others), and business leaders generally accept the need for privacy programs in their organizations. We are no longer debating whether we should implement privacy programs; we are only asking “How is it done?”

We believe that our management model, ***Privacy by 3PT***[®], is useful in answering this question. This model is named for its four major components – *people, policies, procedures, and technologies*. These components create a comprehensive model for the design, development, implementation, monitoring, and assessment of privacy programs. This privacy model specifically differs from security models in that it emphasizes behavioral requirements supported by technology. Conversely, security models generally emphasize technical requirements supported by behavior.

² i.e., “*Underlying Technical Models for Information Technology Security*”, Gary Stoneburner, National Institute of Standards and Technology, Department of Commerce, US Gov’t Printing Office, December 2001.

Our **3PT** model initially examines the roles people play because it is primarily a privacy model more than it is a data protection model, and the latter is largely served by available security models. Privacy, on the other hand, has few if any management models sufficient to cover all the complex needs presented by responsible management of personal information in complex environments. To our knowledge, none deals directly with personal behaviors.

We start, therefore, with people. As in any policy space, there are multiple dimensions to each facet of the issue, and so it is with people. A robust privacy program has to account for the interactions between different kinds of data subjects and types of data controllers who in turn may employ various classes of data processors. For example, a child interacting with a Web site sponsored by a breakfast foods company presents different policy and staffing requirements from those involved when a senior citizen interacts with a retailer selling pharmaceuticals. In each case the data definitions, the policy considerations, the communications, and staff training are significantly different. There is no formula whereby a single sweeping set of criteria apply universally.

The facet of the model called 'People' focuses on several critical challenges. It requires that the data subjects, controllers, and processors are accurately described, that the data is appropriately classified and that the roles in the data controller and processor organizations are described in detail. Often, this facet involves the identification of workers in specific roles and the development of their knowledge and skills. This and all facets of the model are supported by a series of process

methodologies we refer to as lifecycles. The lifecycles involve completing specific processes designed to accomplish discrete goals and outcomes. For the 'People' facet, each lifecycle has a distinct contribution. We will discuss the lifecycles more fully later.

The 'Policy' facet of the model focuses on the many concerns presented by corporate values, commercial requirements, legal regulations, and market demands. This facet is designed to produce over-arching positions that are consistent with business strategies, meaningful to constituents, and acceptable to regulators. The Policy facet is directly supported by a process that develops, assembles, and documents these fundamental positions and aspirations. It is also supported by other methods, including the Communications lifecycle, which focuses on broad awareness and specific training.

In the Procedures facet of **3PT**, we concentrate pragmatic work issues; it is the most task-oriented facet and requires the most work effort to support. For the Procedures facet, we document the way information is brought into, is processed by, and eventually exits an organization. At each step, the information has to exist within a rich environment motivated by clear rules and guidelines to accomplish the desired outcome. The Procedures facet is supported by lifecycle processes that define roles, data, practices, formats, and rules. It is also supported by a Communications lifecycle designed to inform "the right person using the right channel at the right time".

The fourth facet of the **3PT** model, Technologies, recognizes that technical developments including electronic point of sale data input, centralized data processing and the Worldwide Web have created digital information that is easily collected, shared,

and used. These same technical developments that are widely seen as exacerbating our privacy concerns also provide valuable privacy solutions. Most of the technical support for data protection comes from tools and software used in data security; encryption, authentication, identification, threat analysis, and other security procedures promote and ensure data protection. The Platform for Privacy Preferences (P3P) is a technical specification aimed at providing machine-readable support for disclosure practices. Advances in structured database rules like IBM's Tivoli are showing real promise in integrating policies at the level of the data itself. Microsoft's promised digital rights management software may be applicable to personal information protection. Software for Web monitoring like those offered by Watchfire detects rules violations in online environments. Technical means for promoting anonymity like those developed by Zero-Knowledge have promoted individual control. These and other technology developments are beginning to emerge as privacy-enabling technologies (PETs) that support data protection objectives. More than any other, this facet of our model brings together Security and Privacy practices and objectives.

As mentioned, each facet of the ***3PT*** model has associated implementation method and steps. We refer to these methods as lifecycles because they are processes rather than destinations and they tend to cycle back on themselves in a continually renewing way. Thus, each lifecycle method involves a feedback loop aimed at informing regular analysis and updates.

The lifecycle methods and steps include:

- Vocabulary –a method for defining system resources, creating a data dictionary, detailed employee roles, security & privacy concepts, interface formats and information management rule sets
- Policies –a method for describing organizational values and principles, infrastructure needs, legal requirements, and information management disclosures and practices
- Communications –processes for expressing policies and roles, creating awareness and training programs, matching messages to appropriate roles, delivering messages using multimedia/multimodal methods, and assessing communications effectiveness
- Data – the ways information moves into, through, and out of organizations, including collection, storage, use, sharing, retention and disposal
- Activities – procedures to guide the information-driven processes within large organizations such as research, marketing, sales, analysis, worker performance, operations, finance, and infrastructure administration

The steps within each lifecycle method are applied to each facet of the 3PT model for each of at least three communities – individual consumers, employees, and business partners. These communities may be simple or complex. For example, an employee privacy model might include contract workers, workers in affiliate organizations, and workers in unaffiliated vendor organizations in addition to direct employees.

Privacy by 3PT[®] is particularly useful in large organizations with multiple locations. It is the only management model that can incorporate cultural and legal norms and standards within a consistent framework. It is also the only model that promotes centralized management, local accountability, reliable monitoring, and consistent reporting. Because it allows flexibility within different jurisdictions without changing the overall framework of the model, it promotes adaptation and application in varied circumstances. This flexibility still maintains consistency in applying privacy protections and data security controls both within the organizations and within its marketplaces. ***Privacy by 3PT[®]*** provides value to executives, shareholders, business partners, and consumers. The real beneficiaries, though, are the privacy professionals who are accountable for privacy programs in their organizations. This model provides a solid basis for them to build sustainable programs that will ultimately become woven into the fabric of commercial operations.