Privacy is a Process, not a PET
A Theory for Effective Privacy Practice

Anthony Morton
University College London
Department of Computer Science
Malet Place, London, WC1E 6BT
Tel: +44 (0)20 7679 2788
anthony.morton.09@ucl.ac.uk

M. Angela Sasse
University College London
Department of Computer Science
Malet Place, London, WC1E 6BT
Tel: +44 (0)20 7679 7212
a.sasse@cs.ucl.ac.uk

ABSTRACT

Privacy research has not helped practitioners – who struggle to reconcile users' demands for information privacy with information security, legislation, information management and use – to improve privacy practice. Beginning with the principle that information security is necessary but not sufficient for privacy, we present an innovative layered framework - the Privacy Security Trust (PST) Framework - which integrates, in one model, the different activities practitioners must undertake for effective privacy practice. The PST Framework considers information security, information management and data protection legislation as *privacy hygiene factor*s, representing the minimum processes for effective privacy practice. The framework also includes *privacy influencers* - developed from previous research in information security culture, information ethics and information culture - and *privacy by design* principles. The framework helps to deliver good privacy practice by providing: 1) a clear hierarchy of the activities needed for effective privacy practice; 2) delineation of information security and privacy; and 3) justification for placing data protection at the heart of those activities involved in maintaining information privacy. We present a proof-of-concept application of the PST Framework to an example technology – electricity smart meters.

Categories and Subject Descriptors

H.1.2 [User/Machine Systems]; Human factors; K.4.1 [Public Policy Issues]: Privacy.

General Terms

Management, Design, Security, Human Factors.

Keywords

Privacy, trust, security, framework.

1. INTRODUCTION

In his 2004 book, *Secrets and Lies*, Bruce Schneier describes how, after writing *Applied Cryptography*, he "*learned to look beyond the cryptography, at the entire system, to find weaknesses*." [58]: he observed that weaknesses are often caused by hardware, software, networks and people, and not failures in cryptographic mathematics. He concluded that: 1) "*Security is a chain; it's only as secure as the weakest link*"; and 2) "*Security is a process, not a product*" [58].

Over the past decade, information security researchers and practitioners have recognized that human behavior is a major potential source of vulnerabilities, and organizations have started to understand that information security is more than a collection of physical and technical controls – it must be considered and managed as a socio-technical system. We argue that, although technology plays a vital part in safeguarding privacy, a similar holistic approach is required to deliver effective privacy practice.

The UK Information Commissioner's Office agrees - it suggests the need for a *privacy by design ecosystem* "[...] *to ensure that privacy becomes embedded not only in all aspects of the systems lifecycle, but for organisations becomes part of 'the way we do things around here'.* [...] *Within each organisation, the mandate will need to spread down from executive management throughout the organisation, being delivered as policies, standards and implementation guidelines"* [68]. Cavoukian proposes the idea of *SmartPrivacy* [18], augmenting *privacy by design* (PbD)[1] [14, 16], to include law, regulation, market forces, education and awareness, independent oversight, fair information practices etc. Whilst these approaches identify elements that should be considered, they do not provide practitioners with a single framework for planning and maintaining for information privacy.

The fair information practices referred to by Cavoukian relate to generic guidelines setting out the principles of fair collection and use of personal information, whilst providing privacy protection for individuals. Practical expressions of these principles are found in the US Department of Homeland Security's *Fair Information Practice Principles* [69][2] and the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [34]. These principles also underpin data protection legislation, e.g. the European Union's Data Protection Directive [29]. We take *fair information practices* to mean the general principles – encompassing notice, consent, access, quality and integrity, transparency, purpose specification, data minimization, appropriateness, security, accountability and auditing when collecting and processing personal data.

[1] See http://privacybydesign.ca for further information.

[2] The US Department of Homeland Security's *Fair Information Practice Principles* are more extensive than the US Federal Trade Commission's *Fair Information Practices in the Electronic Marketplace* [30], which contain only notice, choice, access and protection, and security, and were criticised for being watered down [32].

Privacy research has made considerable progress in terms of understanding privacy economics, people's privacy concerns, behavior and decision-making, and the effect of technology design. However, there has been no attempt to create a framework that unifies the insights from research on privacy, information security and trust, and represents the composition of privacy of the parties involved in a technology-mediated interaction. Practitioners currently struggle to figure out how to reconcile privacy with information security, governance, data protection legislation, trust, and information management and use. With increasing legislative pressure and consumer awareness of privacy, practitioners face the challenging task of understanding how to meet data protection laws, maintain consumer trust and ensure operational security – all at the same time.

The Privacy Security Trust (PST) Framework presented in this paper models the composition of the privacy practice of the parties in a technology-mediated interaction, the construction of the trust between them, and the characteristics of the technology involved. The objective of the PST Framework is not to explain privacy behavior, or the motivations of individuals and organizations, but to help deliver good privacy practice by providing: 1) a clear hierarchy of the activities needed for effective privacy practice; 2) delineation of information security and privacy; and 3) justification for placing data protection at the heart of those activities involved in maintaining information privacy.

To overcome the definitional complexities surrounding privacy [25, 62] the PST Framework focuses on information privacy. However, information privacy is not a binary construct: what is considered sensitive, or private, information varies between individuals, and depends on factors such as information usage, context and the perception of the information receiver (e.g. "*Who or what has access to my personal information?*") [2, 3, 7, 8]. Privacy is also temporal: sensitivity of information may change over time, e.g. an individual's willingness to disclose their age. A definition of information privacy must therefore address the contextual nature of privacy, its dynamism, and the use to which information is put.

Using Solove's [62] *taxonomy of privacy problems*, Westin's [73] control-based definition of privacy, and considering the non-binary nature of information privacy, we define information privacy as "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information they consider sensitive at a prescribed point in time is collected, processed, stored* [3] *and communicated to others, within a given context*"; for clarity the remainder of this paper uses *privacy* to refer to *information privacy*. This idea of informational self-determination underpins fair information practices, and hence European data protection laws, even though in practice, fair information practices typically depend upon "*procedural protections*" [6].

This paper initially considers the principal prerequisites for privacy and the influences upon it. It then describes existing frameworks for privacy, information security and trust in technology-mediated interactions, and sets out some of their shortcomings. We then examine three additional areas of work relevant to the PST Framework: information culture, information ethics and PbD. We then describe the PST Framework in detail, particularly its innovative use of a layered approach to privacy. Finally, we present a proof-of-concept application of the PST Framework to an example technology – electricity smart meters.

2. HYGIENE FACTORS & INFLUENCERS

Camp [13] argues that privacy requires security, because privacy is the ability of the subject of the information to control the information, and security is required to maintain control over information. An information security failure is one of the more obvious reasons for the inadvertent disclosure of private information; as recent examples show [53, 67], i.e. "*data breaches as a privacy problem*" [22]. Thus, the information security practice of the party being trusted (*trustee*) with sensitive information in a technology-mediated interaction is one of the factors in the decision by the trusting party (*trustor*) to trust it. However, "*security is not sufficient for privacy, since the owner and the subject of the information may have different interests in and uses for the data.*" [13]. Therefore sound information security practices are necessary, but not sufficient, for privacy.

If information security practices are a prerequisite for privacy, they become a *privacy hygiene factor*. Another key *privacy hygiene factor* is legislation pertaining to privacy and data protection - representing the 'letter of the law'. Examples include the sector-specific approach in the US, such as the Health Insurance Portability and Accountability Act 1996 (HIPAA) and the 1970 Fair Credit Reporting Act, and the more comprehensive protections of the UK Data Protection Act 1998 (UKDPA), which cover information collection, access, use, storage and dissemination. Legislation, such as US sector-specific statutes and the E.U. Data Protection Directive, establish a regulatory floor, shape compliance-oriented measures, and justify trustees' initial commitment of resources to safeguarding customers' privacy [6]. However, legislation can play a limited role in defining what information privacy means for organizations [6].

Camp argues that "[r]*eliability, security and privacy are critical in* [Internet] *commerce systems*" [13], and that reliability and security are interdependent. This excludes the critical role of sound information management practices as a *privacy hygiene factor*. The fact that "[…] *the control of information enabled by security does not imply privacy"* [11], suggests a trustee requires other mechanisms to ensure privacy. One such mechanism is the ability to manage information effectively, so a trustee is aware of the location and status of the information it is responsible for; this is particularly important for meeting legislative requirements pertaining to information collection and processing. For example, under the UKDPA, effective information management practices are required to efficiently handle Subject Access Requests. This suggests a set of privacy hygiene factors, representing a minimum set of activities for effective privacy practice (lower half of Figure 1).

The top half of Figure 1 shows *privacy influencers*, which include information culture [20, 21] and information ethics [22, 59, 61]. These shape how a trustee manages and uses information – its privacy behavior. For organizations, this privacy behavior [19] underpins organizational trust, one of the key determinants of trust - a trustor is more likely to trust an organization exhibiting good privacy behavior. Information use, identified as an important factor in a user's decision to engage in a technology-mediated interaction [2], is another privacy influencer, along with the information principles used to guide a trustee's information use decisions.

[3] Information storage is not identified in Solove's '*taxonomy of privacy problems*'.

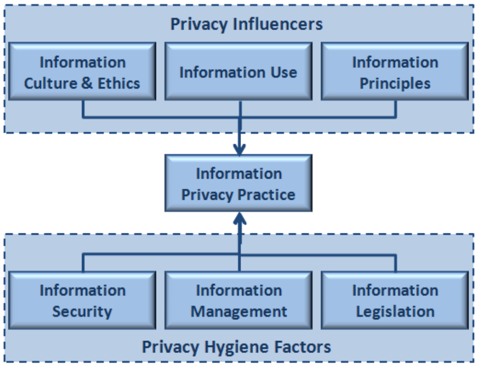

Figure 1. Information Privacy Practice Hygiene Factors and Privacy Influencers

An organization's information principles will be based on applicable information legislation, but are likely to extend it, so that an organization's information privacy practice encapsulates data subjects' expectations of its privacy behavior. For example, under the UKDPA a court may order an organization to rectify, block, erase or destroy all inaccurate data it holds on a data subject. However, organizations may choose to exceed this, e.g. by ensuring its technology platform and information management processes allow customers to view, amend and delete all information the organization holds about them. In essence, if the privacy hygiene factor *information legislation* refers to the 'letter of the law', the privacy influencer *information principles* represents the 'spirit of the law'.

Information management requires information security to ensure its information-sharing decisions are carried out correctly. An organization's approach to information management is determined – in turn - by information principles and organizational characteristics (e.g. its culture and ethics). A potential hierarchy therefore begins to emerge, flowing from a trustee's softer influencing attributes (*privacy influencers*), such as information ethics, information culture and information principles, down to the concrete legislative requirements, information management practices and information security (*privacy hygiene factors*).

3. EXISTING FRAMEWORKS

3.1 Users' Privacy Perceptions

Adams & Sasse [2] introduced a model of the principal factors forming users' privacy perceptions when engaging in a technology-mediated interaction (Figure 2). The model shows the relationships between the three principal privacy factors considered by a user for a given context: *information receiver* (the entity receiving the information); *information usage* (what the *information receiver* will use the information for); and *information sensitivity* (the user's own perception of how sensitive the information is). The model also illustrates the relevant privacy issues: *trust* in the *information receiver*; the *risk or benefit* of *information usage* (i.e. privacy cost *vs.* benefit trade-off); and the user's *judgment* concerning *information sensitivity*.

This model was originally developed to explain privacy issues in multimedia communication [1], but it can be applied to other technology-mediated interactions where a trustor (user or *information sender*[4]) decides to trust a trustee[5] (*information receiver*), and engage in a technology-mediated interaction within a given context. For example, the model can be used for a scenario in which an *information sender* (e.g. customer) submits personal financial information to an *information receiver* (e.g. financial services organization), within the context of a credit card application. In this example, the *information sender's* expected *information usage* is to support their credit card application, with the *information sensitivity* likely to be high (e.g. salary information, employer name and address, credit history etc.).

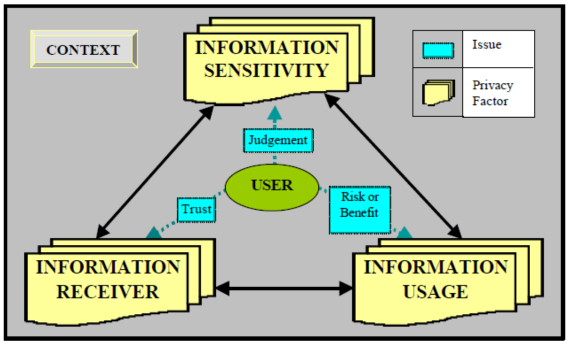

Figure 2. A User's Privacy Perceptions. Source: [2][6].

In the case of applying for a credit card, an individual's expected *information usage* will be dictated by two informational norms: 1) *information appropriateness* (e.g. requesting information concerning an applicant's credit history is acceptable, but not their medical history); and 2) *information distribution* (e.g. information is sent to a credit reference agency, but not an e-commerce vendor who targets the individual with adverts) [50]. Preventing the violation of customers' privacy expectations concerning information use and reuse – "*a harm avoidance approach"* – can play an important role in developing organizations' privacy practices [6].

Adams & Sasse's model captures the principal components of information privacy in technology-mediated interactions. However, it does not cover: 1) different types of information usage; 2) unauthorized information usage by third parties; 3) the process by which an information sender trusts a technology and information receiver; and 4) the impact on individuals' privacy perception of passive *vs.* active data collection.

3.2 Information Security

There has been a growing realization amongst researchers and practitioners that effective information security is more than a collection of physical and technical controls. Those responsible for an organization's information security have to be cognizant of the threats from social engineering [9] and the (in)action and behavior of employees [27]. Information security therefore requires a security-aware socio-technical system with employee involvement, awareness and commitment [70].

The paradigm shift of seeing information security as a socio-technical system has led to the idea of greater integration between research in information security and organizational culture, and

[4] An *information sender* equates to Adams & Sasse's *information broadcaster* [2].

[5] Assuming the trustor is in a position to actively choose whether or not to trust the trustee.

[6] Original diagram source: Adams, A (2001) *Users' Perceptions of Privacy in Multimedia Communications*, University College London [1].

the concept of information security culture [43, 65, 70, 71]. An information security culture is one in which information security skills become part of employees' everyday practice, with the aim of reaching a point where information security culture is indistinguishable from organizational culture [65].

There have been significant advances in information security practice, both in terms of addressing human security behavior, and closer integration with business objectives and legislative requirements. Nevertheless, there are still two shortcomings in terms of information security's relationship with privacy: 1) an inability to clearly articulate the relationship between data protection legislation, security and privacy; and 2) the need to better understand the influence of information security culture on privacy.

Practitioners currently have little guidance on how to map data protection legislation onto information security and privacy safeguards and practices. Despite increasing recognition that information security is a socio-technical system, there is still an emphasis on protecting data through the implementation of information security management systems in accordance with standards such as the ISO/IEC 27000, as well as adherence to data protection legislation. So in most organizations, data protection is the responsibility of Information Security Departments. This data-centric view of data protection will cause problems for organizations as customers demand greater control over their personal information, and privacy becomes a point of differentiation for customers when selecting organizations to transact with.

Adams & Sasse argued - because privacy breaches can have a serious impact on individuals' lives - effective privacy protection is about more than protecting data [2]. Safeguarding individuals' privacy requires organizations to not only adhere to data protection legislation and provide a minimum level of privacy, but also free data protection from its current tight coupling with information security, placing it at the heart of an organization's principles for handling customers' information. We argue that current approaches to data protection and information security do not facilitate such an approach.

If "[a]*n information security culture can be defined as the way things are done in an organisation to protect information assets"*[70]*,* the information security culture of an organization is likely to significantly affect its attitude to, and protection of, the privacy of those entrusting it with their information.

3.3 Trust

Camp observed that "*operational definitions of trust require a party* [(trustor)] *to make a rational decision based on knowledge of possible rewards for trusting and not trusting* [a trustee]". She also suggested that "*trust is an element of all systems*" [11] and proposed a three-dimensional definition of trust, constructed from a trustee's intent and competence in providing reliability, security and privacy [13]. However, this does not explain the role of the privacy hygiene factors information management and adherence to legislation, as well as the role of privacy influencers in building a trustor's trust in a trustee's information privacy practice.

A trustor engaging in a technology-mediated interaction is likely to have assumptions and expectations of the technology and trustee's privacy behavior. These may be influenced by *trust signals* emitted by the trustee, allowing a trustor to determine if trust should be given when engaging in a technology-mediated interaction [56]. These *trust signals* include *trust symbols* (e.g. use of HTTPS and trusted third party seals), and *trust symptoms* (e.g. user reviews, professionalism of web site design and usability) [56], as well as previous offline experience, societal norms, and the trustee's reputation. Similarly, stated compliance with privacy-specific regulatory regimes signals privacy leadership to customers and business partners, hence engendering trust [6] – privacy is *"a core value associated with trust"* [6].

If a trustor's experience of a trustee, or technology, does not match their privacy expectations and assumptions, because of a malicious trustee, error or badly designed technology leaking sensitive information, the trustor is likely to feel its privacy has been invaded and reject the technology and/or the trustee [2, 3].

There are two determinants of trust in a trustee's ability to protect privacy: operation of the technology and privacy behavior of the trustee. The relationship between privacy and trust, and peoples' reaction when the privacy behavior of a trustee does not match their expectations, is illustrated by the reaction of US consumers to corporate privacy breaches in the late 1990s – ultimately leading to organizations abandoning plans for information sharing deals [6].

Trust research has provided researchers with insights into the construction of trust– particularly in technology mediated interactions [31, 48, 55, 56, 75]. However, there has been a lack of guidance for practitioners. Riegelsberger *et al.* [56] provided a framework for understanding how trust between trustor and trustee is constructed, and identified the role of trust symptoms and trust symbols. This needs to be integrated with privacy and information security culture in a single comprehensive framework. Furthermore, if trust has two principal determinants – technological trust and organizational trust - the privacy characteristics of a technology and the privacy behavior of the trustee must be represented.

A practitioner needs an answer to the question, "*What activities do I need to perform to safeguard the information privacy of my customers and adhere to data protection legislation, and how will these activities affect the trust my customers have in me?*" Existing trust frameworks have only provided a partial glimpse of what is required to address this question.

4. OTHER RELATED WORK

There are three additional areas included within the PST Framework:

1. **Information culture**: The influence of an organization's information culture on its information collection, use, management and dissemination.
2. **Information ethics**: How organizations make decisions concerning information collection, use, management and dissemination whilst balancing an individual's privacy rights and concerns with organizational objectives - particularly those decisions the organization has not made before.
3. **Privacy by design (PbD)**: The embedding of privacy awareness throughout all stages of a technology's design and implementation lifecycle.

4.1 Information Culture

Information culture, like privacy, is a term "*frequently used but without consensus as to its definition"* [23]. Most researchers agree that it relates to the behavioral patterns, values, norms and attitudes of an organization concerning the value and use of information in achieving its operational and strategic objectives [20, 21, 23, 24]. Pragmatically, information culture consists of: "*communication flows, cross-organizational partnerships, internal environment (cooperativeness, openness and trust); information systems management; and processes and procedures*" [20].

Curry & Moore's [23] exploratory conceptual model attempts to capture the evolution and components of an organization's information culture in terms of people, processes and information, and illustrates how information culture affects, and is affected by, organizational culture. They suggest an organization should aim to reach a point at which its "*information culture is no longer distinguishable from the organizational culture*" [23] – reminiscent of the objectives of information security culture [65].

There has been some research on how firms treat sensitive information, and their organizational privacy behaviors [19, 22]. However, further investigation is required on the specific effect of information culture on organizations' attitude to privacy. Information use plays a critical role in safeguarding a user's privacy [2], and information culture has a significant influence on information use outcomes [21].

4.2 Information Ethics

Organizations often face ethical dilemmas [59] when their existing information management principles or rules do not adequately address a new requirement for information collection, use and dissemination. These "*moments of truth*" [44, 45] often result from increased demand for the collection, storage, dissemination and retrieval of information, as well as the technological imperative of society's desire for progress [45]. A principal cause of this has been the rise of customer-centered interaction as a competitive advantage, necessitating the collection and processing of increasing amounts of personal data [10]; organizations' decision making process when faced with such ethical dilemmas is the focus of information ethics.

If an organization's management is not aware of the existence of ethical dilemmas concerning its information collection, use and dissemination, or it is preoccupied with more pressing operational matters [59], a situation is likely to arise in which its employees' compliance with the organization's privacy policies drifts - perhaps due to commercial or resource pressures - until finally the threat of legislative action forces the organization to act [60]. This leads to emotional dissonance because individual employees face their own ethical dilemmas when there is insufficient guidance by the organization's information principles and guidelines, and they are often reluctant to challenge an organization's ethics [60]. Even when an organization imposes certain rules, ethical decisions are still often "*left to an individual to decide which norms and standards will guide his or her ethical argumentation.*" [59].

Bamberger & Mulligan [6] argue that evidence from their investigation of corporate privacy practice shows that even in the absence of comprehensive privacy and data protection legislation, an organization's information culture, information ethics, and the embodiment of the 'spirit of the law' in its information principles can still lead to the creation of effective privacy practice. They further suggest that despite the patchwork sectoral approach to privacy legislation in the US, e.g. HIPAA, the 1970 Fair Credit Reporting Act and the 1974 Privacy Act, corporate attention to privacy has increased since 1998, exemplified by organizations' desire to meet customers' expectations and prevent substantive harms to their privacy, and the establishment of direct privacy leadership, e.g. the creation of Chief Privacy Officer (CPO) roles. Organizations' privacy practices have still been driven to some extent by a form of regulatory pressure from state data breach notification statutes, and the Federal Trade Commission (FTC) - who has emerged as an activist privacy regulator – with its statutory mandate to police, with considerable discretion and unpredictability, "*unfair or deceptive acts or practices*" [6].

The relationship between privacy, data protection and privacy legislation, and ethical decision-making is further strengthened when one considers that the ethical issues relating to information use are often categorized into: 1) privacy – the ability of people to control the dissemination of sensitive information; 2) accuracy – the quality and accuracy of information held; 3) property – information ownership and control; and 4) accessibility – access to information held [10].

Most organizational privacy violations can be categorized as information re-use and unauthorized access to personal information – the former legal (if not necessarily ethical), and the latter in violation of laws or corporate policies [22]. If prevention of unauthorized access is one of the principal roles of information security, the role of information ethics is to ensure decisions about information re-use are made within an organizational culture that aims to avoid substantive harm to peoples' privacy [6]. Information use decisions are underpinned by an organization's ethical decisions, which can enhance or damage its reputation - hence the trust individuals place in it.

4.3 Privacy by Design

When an individual interacts with another party via a technology platform, and this leads to an invasion of the individual's privacy, they may reject the technology platform and/or the other party [2]. Such privacy invasions can be the result of:

- technology being designed or deployed unethically [8], as suggested for some peer-to-peer (P2P) software [64]; or
- technology being designed without privacy and security uppermost in the mind of the designers and implementers. This results in the user being presented with a confusing interface, and little or no control over their privacy [33].

To address these technology design issues and ensure privacy protection is embedded throughout all stages of a technology's design and implementation lifecycle, PbD – with its Seven Foundational Principles [15] - was developed to ensure that the collection, use and dissemination of information by technologies adhered to fair information practices.

PbD emerged from work on Privacy Enhancing Technologies (PETs) [14]. Since then, further research has been undertaken in this field [16, 40, 41]. The UK Information Commissioner published a report on the subject [68], and the European Commission's plans for revising the European Union's Data Protection Directive has mentioned the potentially important role of PbD in establishing safeguards and mechanisms to make data protection more effective [28].

In 2009 Cavoukian reported [18] that her view of PbD's scope had expanded to include business practices, and physical design and infrastructures, as well as information technologies - so called *SmartPrivacy*. This wider scope is particularly welcome given the discussion earlier in this paper on the impact of an organization's information culture, ethics and security on privacy.

5. THE PST FRAMEWORK

5.1 Overall Structure

The PST Framework (Figure 3) is constructed from the notion of an *information sender* engaging in a technology-mediated interaction with an *information receiver* via a technology platform. In the PST Framework the technology platform is referred to as a *technology lens* to highlight that when an *information sender* views an *information receiver* through a poorly implemented or designed technology platform, they may experience a distorted view of the *information receiver* – no matter how well-intentioned the *information receiver* may be. The socio-technical system of a *technology lens* and *information receiver* constitutes a *technology service.*

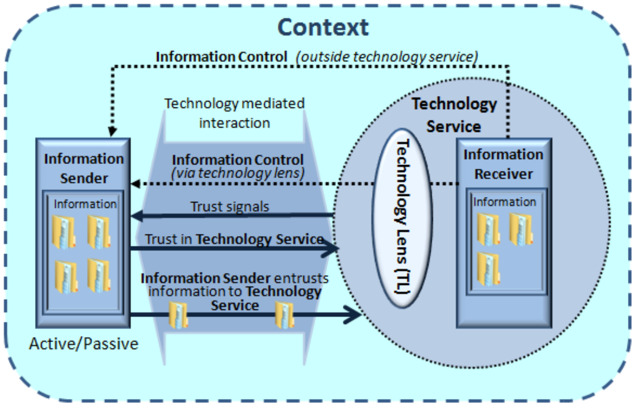
Context
Information Control (outside technology service)
Technology mediated interaction
Technology Service
Information Sender
Information Control (via technology lens)
Technology Lens (TL)
Information Receiver
Information
Trust signals
Information
Trust in Technology Service
Information Sender entrusts information to Technology Service
Active/Passive

Figure 3. PST Framework Components

Table 1 shows five examples of how the PST Framework can be used to represent technology-mediated interactions. Although it is natural to assume an *information sender* is an individual (e.g. e-commerce website customer), and an *information receiver* is an organization (e.g. e-commerce retailer); the last two examples in Table 1 show the PST Framework makes no such assumption.

Table 1. Example Mapping of PST Framework Components

	Technology Service	
Information Sender	**Technology Lens**	**Information Receiver**
Consumer	Shopping web site	Online retailer
Individual in premises	CCTV cameras and recording equipment	Premises owner or manager
Electricity consumer and/or household	Smart electricity meter	Electricity company
Small business	Online business-to-business ordering system	Wholesaler
P2P user	P2P file-sharing client	P2P user

There will be occasions when an *information sender* is not able to choose if they wish to interact with a *technology service*; for example:

- When use of a *technology service* is mandatory. For example, an *information sender* has to use a web site to provide their personal information when travelling to the United States and some European countries.
- An *information sender* may be unaware they are engaging with a *technology service*, e.g. the positioning of a webcam in a 'public' space, such as a staff common room, without clear notification [3].
- An *information sender* may not possess sufficient specialist knowledge to allow them to understand when they may be passively engaging with a *technology service*, e.g. the placing of tracking cookies on a user's PC when they visit a web site.

When individuals discover they have been unwittingly engaging with a *technology service*, they may respond emotionally and reject the *technology lens*, and/or distrust the motives of the *information receiver* [2, 3]. In both instances the *information sender* is a passive subject of data collection, which is likely to significantly increase their privacy concerns.

In the case where the *information sender* actively chooses to engage with a *technology service*, *trust signals* [56] received from the technology service, prompt the *information sender* to decide to entrust the *technology service* – hence the *information receiver* – with information, some of which the *information sender* may consider sensitive. In essence, "[…] *the final placement of trust is illustrated by a willingness to share personal information*." [11]

The *technology lens* should be considered a virtual technology platform, as it is likely to consist of multiple computer systems; in the case of e-commerce it will include a web server farm, application servers and back-end databases – potentially geographically distributed. An *information sender* will not make a distinction between these different computers - viewing them as an homogenous system [12] - but will simply decide whether to trust the combination of *information receiver* and *technology lens* - the *technology service*. This is particularly important in terms of trust and forgiveness - Camp *et al*. hypothesized that there is "[…] *no significant systematic difference in people's reactions to betrayals that originate from human actions, on the one hand, and computer failure on the other*" [12]. People are therefore unable to differentiate between privacy breaches caused by technology failure and those due to human actions within a *technology service* - was it a failure in technology or human agency which resulted in the Sony PlayStation breach [53]?

Figure 3 shows *information control*, which the *technology service* provides, allowing the *information sender* to control the flow of information to the *information receiver*. For example, the ability to easily and intuitively control access to shared data is of particular importance in collaborative environments [7]. *Information control* may be via the *technology lens*, e.g. through technical design features allowing the *information sender* to: opt-in or opt-out of the *technology service*; select which information to provide to the technology service; and view the information the *information receiver* has access to. The *information control* provided by an *information receiver's* internal systems and processes should flow seamlessly through the *technology lens* to the *information sender*. Failure to achieve this may cause well-intentioned attempts to provide the *information sender* with the functionality to control their information flow, to be omitted or distorted by a poorly implemented or designed *technology lens*. As shown in Figure 3, *information control* may occur outside of the *technology service*, through mechanisms such as the UKDPA's Subject Access Request or HIPAA's Privacy Rule, or communicating directly with the *information receiver*, e.g. requesting a customer account to be deleted.

There may be situations in which there is more than one *information receiver* - some of whom may not be known to the *information sender*. This is provided in the PST Framework by allowing an *information receiver* to be an *information sender*, either simultaneously or at a later point in time. For example, in a CCTV system an *information sender* (e.g. an individual working in a street market) has information captured in the form of images of herself working in the market and sent to an *information receiver* (e.g. local government authority). In this particular example the *information sender* is a passive actor, although they may be aware that image recording is taking place because of street signs explaining the *information receiver's* intended use of the information (e.g. ensuring the safety of the public). If a central government agency (e.g. social services) subsequently seizes the CCTV tapes, the local government authority becomes an *information sender*, with the central government agency as a secondary *information receiver*. The central government agency may then use the images for another purpose, such as detecting benefit payment fraud.

5.2 Technology Service

The socio-technical nature of a *technology service* emphasizes the point that - to fully understand the privacy impact of a technology - it is necessary to not only consider the core technologies involved (e.g. hardware and software), but how those technologies are implemented, and the organizational processes, principles and culture surrounding them, i.e. the context in which the technology service is operating also requires consideration. For example, a technology service that embeds an RFID chip in a patient to track them and monitor their health whilst in hospital may be considered acceptable from a privacy point of view. The same technology service used outside of the context of a hospital may be viewed as unacceptable. Bellotti & Sellen suggest, "[t]*echnology is not neutral when it comes to privacy.*" [8], but we argue that a core technology cannot automatically be considered privacy-invasive; it is the manner or context in which it is used which determines this.

An example of how a technology in itself should not be considered privacy-invasive is the use of RFID in product tags attached to items in a retail outlet. RFID tags can be managed in accordance with robust security and privacy processes by permanently disabling them with the appropriate *kill* command at the checkout. In this scenario, most observers would not consider them to impact on their privacy. However, if the RFID product tag was not disabled, or was sewn into a garment unbeknown to the wearer, and they then received offers for similar products when visiting other stores, this would be considered by most to be an infringement of their privacy. This example highlights the importance of considering not only the core technologies themselves, but their mode of implementation, the organizational processes surrounding their implementation and continued operation, and the objectives (worthy or otherwise) of the organization deploying the technologies.

5.3 Component Definitions

Before progressing further it is prudent to formally define the components within the PST Framework.

5.3.1 Information Asset (IA)

As shown in Figure 3, the information receiver and information sender possess information, which are considered as *information assets* in the PST Framework. 'Asset' here is employed in its figurative and extended sense to mean "*a thing, person, quality, etc., that serves as an advantage, support, or source of strength*" [51]. Building on this idea of an asset as something of value, *information asset* has been defined as "*knowledge or data that has value to the organization"* [36]. We define *information asset* (IA) as "*information endowed with value, relevance and purpose for an individual, group or organization*".

If an IA is defined as sensitive by data protection legislation, an organization must decide if other IAs should be considered private for all users, or if information control mechanisms will suffice for those IAs considered private by only some users. This echoes the idea of two types of private information [7]:

- **Normative** - information relating to an individual that is inherently private, e.g. medical records.
- **Operational** – information whose sensitivity depends on the individual, e.g. salary.

Pragmatically, IAs should therefore be categorized with one of the following attributes:

- **Non-sensitive** - generally not considered sensitive.
- **Choice-sensitive** – this is the same as Bellotti's [7] operational privacy, i.e. a user can use information control mechanisms to manage their IA flows.
- **Sensitive** – this is the same as Bellotti's [7] normative privacy and is often defined by data protection and privacy legislation, or is generally considered sensitive by most users.

5.3.2 Information Asset Holder (IAH)

Building on the definition of an IA, the information sender and information receiver are each considered to be an *information asset holder* (IAH). We define an *information asset holder* as "*an individual, group or organization which possesses one or more information assets*". This definition is kept broad to cover individuals, groups and organizations, as well as recognizing that the IAs an IAH holds, may consist of those it owns as well as those entrusted to it by other IAHs.

In a technology-mediated interaction, an IAH may act as an *information asset sender* (IAS) or an *information asset receiver* (IAR). For example, an IAH acting as an IAS (e.g. a user filling in a form on a web site) may provide one or more IAs (e.g. address, date of birth, salary etc.) to another IAH acting as an IAR (e.g. a financial services organization using the web site to collect IAs for a credit card application).

Privacy problems can occur when an IAS considers an IA to be sensitive, but an IAR does not, and therefore does not exercise adequate stewardship of the IA.

5.3.3 Technology Lens (TL)

We define a *technology lens* as, "*a technology platform through which an information asset sender - actively or passively - passes one or more of their information assets to an information asset receiver"*.

5.4 Information Asset Holder Layers

5.4.1 Overview

The PST Framework views the provision of privacy by an IAH using a conceptual model similar to the Open Systems Interconnection (OSI) model, which standardizes the functions of a communication system, as performed by the sender and receiver, into layers of abstraction. Within the OSI model each network layer consumes services provided by the layer below, and in turn provides services to the layer above. Similarly, in the PST Framework each IAH contains layers of increasing abstraction (Figure 4), with each layer relying on the layers below to function effectively. When an IAH acts as an IAR, there will be increasing privacy if all layers exist with sufficient attention and resources directed at all layers equally.

Each layer requires the services of the layer directly below it, and influences all layers beneath it. For example, an IAR's *Information Privacy Culture Layer* will not only influence information use and management [20, 21] in the *Information Use Layer* and *Information Management Layer*, but also determine if the principles operating at the *Information Principles Layer* are designed to minimally adhere to legislation, or if they are maximized to genuinely protect the interests of the IAS's who entrust their IAs to the IAR, hence attempting to avoid "*substantive harm*" to an IAS [6].

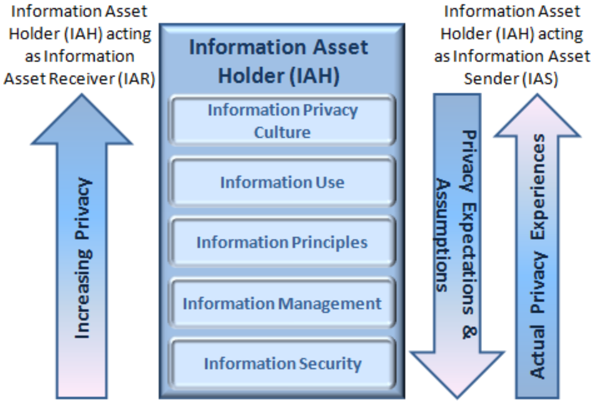
Information Asset Holder (IAH) acting as Information Asset Receiver (IAR)
Information Asset Holder (IAH)
Information Asset Holder (IAH) acting as Information Asset Sender (IAS)
Increasing Privacy
Information Privacy Culture
Information Use
Information Principles
Information Management
Information Security
Privacy Expectations & Assumptions
Actual Privacy Experiences

Figure 4. Information Privacy Layers in an IAH

Not all layers may exist in an IAH, or be only minimally implemented. For example, some degree of privacy is possible if an IAH implements only the *Information Security Layer*, e.g. by encrypting data files. However, privacy is likely to be threatened, as an IAH may find it difficult to manage the IAs in its possession. The IAH may therefore choose to implement the *Information Management Layer*, thus increasing the chance of maintaining privacy.

The balance between technology and human factors alters when moving from the top to the bottom layers of the PST Framework. For example, the *Information Security Layer* will mostly consist of technical security controls (e.g. firewalls, encryption, anti-virus, web traffic filtering etc), surrounded by some human activities in the shape of security management processes (e.g. audit, access management, patching, monitoring and security rules administration). In contrast, the activities at the *Information Privacy Culture Layer* will principally be focused on human factors, such as engendering an information security culture within the IAH. As some controls in each layer are optimally implemented by humans, an IAH must decide, for their particular context, the most suitable mixture of technology, processes and people when implementing effective privacy practice at each layer (e.g. a security guard at the office entrance or biometric authentication).

When an IAH is acting as an IAS and engaging with a technology service it has not used before, an IAS' privacy expectations and assumptions will be primarily focused on the top half of the PST Framework (e.g. trust in the IAR and/or the TL) rather than considering the potential security and privacy risks (Figure 4). For example, an IAS who has never used a shopping web site before may only consider the information privacy culture of the IAR, albeit based on their subjective opinion of the IAR's ethics and culture; in short they will ask themselves, "*Can I trust this organization to look after my information appropriately, and will it behave as I expect?*"

The actual privacy experiences of an IAH acting as an IAS are likely to be focused on the bottom half of the hierarchy (Figure 4). The security breaches of Sony's PlayStation Network [53] - caused by failures in the lower layers of the hierarchy - provide an example of this. Customers signing up for Sony's games networks probably had high initial organizational trust, because of its perceived good reputation. The loss of their personal details because of an information security failure is likely to have decreased their level of trust in Sony. PlayStation users are likely to have generalized broadly from their negative experiences [12], to other Sony technology services and/or other games networks.

Focusing on the bottom half of the hierarchy will not always be restricted to the actual privacy experiences of an IAS. Even when interacting with a technology service for the first time, an IAS – especially when they have some technical knowledge or have received security awareness training - may check for certain types of trust symbols [56] at the *Information Security Layer*, e.g. the existence of an HTTPS padlock on a web site. However, reliance on such trust symbols may lead a user to incorrectly generalize this guidance and assume all websites supporting HTTPS are trustworthy [12].

The PST Framework assumes the privacy layers also exist when an IAH is an individual in possession of IAs. A reasonable criticism of the use of a layered approach for individuals is that their behavior is unlikely to strictly follow a hierarchy, and hence it is not feasible to empirically detect the layers. However, an individual may have sound information principles (*Information Principles Layer*) regarding who has access to information they consider sensitive, but are unable to put these into practice, due to their poor practices at the *Information Management Layer* and *Information Security Layer* (e.g. they use unencrypted USB memory sticks with sensitive information). For the purposes of clarity, we only describe the more usual situation in which the IAH is an organization.

The following five sections describe each of the information privacy layers in an IAH (Figure 4), starting from the bottom. For each layer, a brief description of its function is given, where relevant, an overview of the services provided to the layer above, and an example illustrating typical activities at each layer for an organizational IAH are provided.

5.4.2 Information Security Layer

The Information Security Layer in an IAH protects IAs from threats leading to their loss, unauthorized access, corruption, interruption or unauthorized disclosure, thus providing assurance that any IA sharing decisions the IAH makes are correctly performed. The Information Security Layer provides services for the Information Management Layer, including: secure storage, access control, secure transfer and protection against malware and viruses. In this layer an organizational IAH will operate technical and operational controls, and must therefore have "[b]*oth good intent and technical competence* […] *to ensure security*" [11].

The Information Security Layer with its technical controls and security management processes must be considered a socio-technical system – albeit principally technically focused. It is the combination of this layer and the information security culture component in the Information Privacy Culture Layer (Section 5.4.6), which represents the full scope of the information security socio-technical system within the IAH.

The Information Security Layer must be able to facilitate an IAH's objectives by providing a sufficiently functionally rich set of services to support effective, yet secure, information management processes in the Information Management Layer. If information security is too restrictive, it will inhibit information management and hence impact an organization's ability to achieve its objectives. For example, an Information Security Layer providing secure storage at only one physical location is unlikely to support the information management processes required to achieve an organization's aims.

5.4.3 Information Management Layer

Choo *et al.* define information management as:

> "[...] *the capability to manage information effectively over the life cycle of information use, including sensing, collecting, organizing, processing and maintaining information."* [20]

Following this definition, the Information Management Layer provides the tools and processes which allow an IAH to implement information lifecycle management, by providing control over their IAs in terms of collecting, locating, sharing, archiving, copying, mirroring, deleting, disseminating, backing up and restoring them. More generally, it encompasses the mechanisms (technological and managerial) which allow an IAH to be fully aware at all times of the location and nature of its IAs. At this layer, an organizational IAH may deploy and maintain a storage infrastructure and associated technology management processes suitable for the volume and type of data the IAH has to store and process.

The mechanisms provided by the Information Management Layer should enact the policies defined in the Information Principles Layer, hence complying with the data access and governance requirements of relevant data protection and privacy legislation. An IAR should not only possess information management mechanisms to manage its own IAs, but also provide them via the TL to any IAS that has entrusted it with its IAs.

An important role of the Information Management Layer is to protect information privacy by controlling access by human agents to data by only allowing them to ask pre-determined queries. A practical example of this is a shopkeeper selling alcohol, who should only be able to ask for proof a customer is over a certain age, rather than for their date of birth.

5.4.4 Information Principles Layer

The Information Principles Layer describes the rules which guide an IAH when using IAs. For example, an organizational IAH may have a privacy policy which sets out its general information principles, such as not sharing IAs unless expressly authorized to do so by the IAH to whom the IAs belong.

As suggested in Figure 1, for an organizational IAH this layer can be split into principles concerned with the 'letter of the law' (e.g. meeting legislative requirements) and principles concerned with the 'spirit of the law' (e.g. exceeding legislative requirements or meeting best practices such as fair information practices).

Some organizations may choose to have a thin Information Principles Layer minimally complying with legislative requirements. However, the necessarily generic nature of legislation can cause problems if organizations rely solely on it to guide their privacy practice. The emergence of new technologies, contexts and business models (e.g. increasingly ubiquitous computing such as smart metering and mobile location based services) is challenging the tenets of fair information practices (e.g. notice, consent, security and access) [6]. Organizations can process vast quantities of information willingly supplied by customers, whilst still adhering to the law [6]. Relying solely on legislation may lead organizations to fail to achieve the "*appropriate balance between 'value information flows and being technology-enabled' on the one hand, and 'privacy-centric' or 'trust-generating' concerns on the other.*" [6].

Organizations possessing a "*culture of privacy"* [22], which flows from senior management, goes beyond mere compliance, and includes accountability for privacy, will be better equipped to avoid the financial loss, damage to legitimacy and the wider repercussions resulting from a data breach or misleading reuse and repurposing of information. As one respondent observed in Bamberger & Mulligan's study:

> "[…] *broader principles have to be developed that can guide privacy decisions consistently in a variety of contexts – privacy must be 'strategic, part of the technical strategy and the business strategy.'*" [6]

Organizations with a desire to avoid substantive harm to customers' privacy are likely to develop and implement their own global policies and procedures – *company law* - relating to privacy, and exceeding legislative requirements [6]. This organization-specific 'law' sits between the 'letter of the law' and the 'spirit of the law' within the Information Principles Layer.

As this layer is concerned with principles, it may seem more logical to place it higher in the PST Framework. However, the enactment of information principles at this layer relies on the Information Management Layer directly beneath it, and the Information Use Layer above needs to base its definition of how information is used on the principles set out in this layer.

5.4.5 Information Use Layer

Within the PST Framework, information use is divided into different categories, determined by whether an IAH is acting as an IAS or IAR. When an IAH acts as an IAR the Information Use Layer consists of:

- **Intended information use**: An IAR's intended use for its IAs, as set out in its privacy policy.
- **Advertised information use**: The use of its IAs, which an IAR may describe in its web site or advertising literature.
- **Actual information use:** The actual use an IAR makes of its IAs.

An organizational IAR may set out their *intended information use* in their web site privacy policy. However, because of commercial pressures and technical limitations, an IAR's *actual information use* may differ from the *intended information use* stated in its privacy policy.

The first two types of information use - *intended information use* and *advertised information use* - are considered static in the sense they rarely change. The third type – *actual information use* – should be accurate, timely and easily accessible via the TL. The provision of this information is the *feedback* suggested by Bellotti & Sellen [7, 8], and is required to enable a user to make informed IA sharing decisions at the Information Management Layer of the TL. However, actual information use may only be discovered inadvertently or after the event [3, 33], which may lead to an emotional response and rejection of the technology or IAR [2].

When an IAH acts as an IAS, the Information Use Layer consists of:

- **Experienced information use**: This is the actual information use as experienced by the IAS.
- **Expected information use**: This is based on the assumptions and expectations the IAS has concerning primary and secondary uses of their IAs, which are determined by their understanding of the IAR's intended information use, the IAS's assumptions and expectations of the TL and IAR, and the IAR's advertised information use.

Unlike the types of information use when an IAH is acting as an IAR, *expected information use* and *experienced information use* are not codified, as they are cognitive constructs within an IAS.

The reason for the distinction between *experienced information use* and *actual information use* in the PST Framework is to capture the idea that an IAS can only feel a privacy invasion if they are aware of it (like the example of the staff in the university common room discussed earlier [3]). *Experienced information use* should equal *actual information use*, but an IAS's perception of *actual information use* can be deliberately or inadvertently modified by:

- the TL not providing accurate or timely feedback mechanisms;
- the IAS ignoring or underplaying the effect of actions on their privacy, perhaps due to personality traits or experiences of the IAS; and
- deliberate misrepresentation by the IAR.

This filtering of *actual information use* results *in experienced information use*, which may be a subset of the former, or potentially a disjoint set.

Perceived information usage is one of three privacy factors a user considers when engaging in a technology-mediated interaction, and is an important influence on the privacy risk *vs.* benefit trade-off a user makes [2]. However, the different types of information use described here suggest an IAS is unlikely to be provided with a complete view of information use. This is likely to impact the privacy risk *vs.* benefit trade-offs an IAS makes, as it will be unable to predict the consequences of releasing their IAs.

The misalignment between *expected information use* and *experienced information use* in the Information Use Layer leads to the privacy behavior of a TL or IAR not matching the expectations and assumptions of the affected IAS. As a result, the IAS is likely to experience an emotive response, believe a privacy invasion has occurred, and reject the TL and/or IAR; this leads to a change over time in the privacy perceptions of the IAS - a "*privacy invasion cycle*" [2].

5.4.6 *Information Privacy Culture Layer*

The Information Privacy Culture layer assists the IAH in making decisions about what IAs to collect, store, disseminate and share. It is required when there is no guidance available in the Information Use Layer and Information Principles Layer to direct the decision making processes concerning the use of IAs – these layers being largely responsible for the formation of an organization's privacy and information policies.

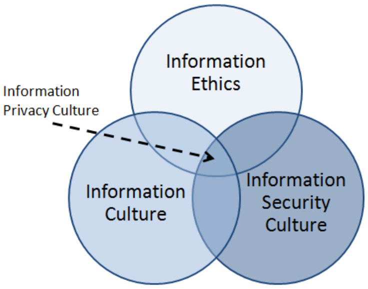

Figure 5. Composition of Information Privacy Culture Layer

If an IAH finds itself facing a decision about the use of an IA for the first time, the decision is likely to be influenced by the IAH's information ethics, information culture, and its ability and desire to protect the IAs entrusted to it i.e. the information security culture of the IAH. We argue that the Information Privacy Culture Layer is therefore created from the intersection of information culture, information ethics and information security culture (Figure 5). This reflects the influence of these areas, whilst recognizing that each encompasses a wider area of influence on overall information management and use within the IAH. We define *information privacy culture* as, "*the ethical position an organization, group or individual, takes with respect to the collection, use, dissemination and disposal of its information assets, particularly when those information assets are considered sensitive by those parties entrusting them"*.

Due to its position at the top of the PST Framework, the Information Privacy Culture Layer influences all attitudes and activity concerned with privacy in the IAR. For example, if an IAR has to make a decision about the use of an IA, this decision may lead to a change in the IAR's information security culture, e.g. if the IAR now has to protect a new type of IA from a potentially new threat, or respond to new technology or market demands for different use of its IAs.

Two studies by Choo *et al.* [20, 21] concluded that information culture in organizations has a significant influence on information use - as opposed to information management. This conclusion aligns with the IAH information privacy layers in the PST Framework, which places the Information Use Layer directly under the Information Privacy Culture Layer, with the Information Management Layer placed further down the PST Framework. In Bamberger & Mulligan's study, CPOs in organizations who set out to meet their customers' privacy expectations, used normative language such as "*values"*, "*ethical tone"*, "*moral tone*" and "*integrity"* [6].

5.5 IAH Layer Pressures

Privacy problems may arise if a layer comes under pressure from other conflicting objectives. The PST Framework assumes the same layers exist in an IAH - irrespective of whether it is acting as an IAS or an IAR - whether it is an individual or organization; this facilitates understanding the impact of these pressures.

Two different technologies are described to illustrate the potential pressures operating at different layers within an individual and organizational IAH:

- **Individual IAH** – The goal of a P2P user is to download media content - possibly pirated. Using the PST Framework highlights how this goal might result in pressures on the individual's Information Security Layer (e.g. installing P2P software from an unknown source), Information Principles Layer (e.g. allowing P2P software to share files in the background might be against the user's normal preference to control which files they share), and Information Privacy Culture Layer (e.g. justifying a weakened ethical position on stealing, when accessing pirated material).
- **Organizational IAH** - The original objective of many CCTV installations in the UK was to reduce crime in city centers. However, there have been numerous cases of local government authorities using the UK Regulation of Investigatory Powers Act (RIPA) to use their CCTV installations to carry out surveillance for minor offences, including littering, dog fouling, and people illegally claiming sickness benefit [63]. This mission creep is often the result of pressure to catch offenders despite resource constraints – using existing CCTV installations offers an easy solution. If the Information Privacy Culture Layer operating in a local government authority does not fully consider the ethical ramifications of doing this, the 'spirit of the law' component of the Information Principles Layer may be compromised, even if the 'letter of the law' component ostensibly follows RIPA guidelines.

The PST Framework is therefore a useful mechanism to consider the likely impact of decisions on privacy – in short, is a decision likely to strengthen or weaken privacy?

5.6 TL Layers

5.6.1 Overview

A similar layered approach to that described for an IAH also facilitates a better understanding of the relationship between an IAR and a TL. It also highlights how activities at a particular layer in an IAR influence the corresponding layer in a TL, e.g. how an IAR's Information Management Layer practices influence the design of the Information Management Layer in a TL.

The next four sections briefly describe the four information privacy layers in a TL, relating them to PbD; as a TL cannot possess an Information Privacy Culture, this layer is omitted.

5.6.2 Information Security Layer

If a TL leaks IAs provided to an IAR by an IAS, the IAS is likely to mistrust or reject the TL and/or IAR [2]. Like the IAH, provision of effective security is a prerequisite for privacy in the TL.

5.6.3 Information Management Layer

A TL should provide information control to an IAS that is integrated fully with the activities in an IAR's Information Management Layer. This layer of a TL should provide the control component in the feedback and control mechanisms required for potentially privacy invasive technology [7, 8]. However, care must be exercised when providing users with control of their personal information, as two of the five designing for privacy pitfalls identified by Lederer *et al.* [41] concern the regulation of privacy:

1. **Emphasizing configuration over action**: The information management provided to the IAS "[...] *requires excessive configuration to create and maintain privacy.*" [41] When an IAS uses a TL to perform an activity, the information management provided by the TL must allow privacy regulation to be "[...] *an embedded component of that activity*." [41].
2. **Lacking coarse-grained control**: An IAS should be provided with the ability to stop and start information disclosure, as well as offering subtle results through use of a small combination of simple controls, rather than complex fine-grained controls [41].

5.6.4 Information Principles Layer

This layer is responsible for ensuring that the design and operation of the TL follows fair information practices, along with relevant data protection and privacy legislation. Langheinrich [40] suggests that "[...] *specific legal requirements such as use limitation, access or repudiation* [...]" (p.288) should be addressed by the design principle of providing mechanisms for access and recourse.

As well as meeting minimum legal requirements, the design of a TL should embody information principles, such as those suggested for ubiquitous computing [40], which aim to create mutual trust and respect between the IAS and IAR; these include:

1. **Notice**: A TL should make an IAS aware of what data is being collected, and for what purpose.
2. **Choice and consent**: A TL should provide an IAS with an explicit option to opt-in or opt-out of data collection and/or services.
3. **Anonymity and pseudonymity**: The design process for a TL should explicitly consider whether an IAS is allowed to remain anonymous or pseudonymous, even if the ultimate decision is not to implement this principle.
4. **Proximity**: A TL should only ask for consent for data collection which typically requires permission.
5. **Locality**: Where relevant, a TL should keep information flows to a restricted geographic area to stop the unnecessarily wide propagation of IAs.

The *Information Principles Layer* in an IAH relies upon the *Information Management Layer* to enact the IAH's principles. Similarly in a TL, technical mechanisms should be provided at the *Information Management Layer* to provide the functionality to implement these design principles.

5.6.5 Information Use Layer

The *Information Use Layer* in a TL should provide technical mechanisms to reflect the information use defined by an IAR's *Information Use Layer*. The TL should achieve this by providing an IAS with feedback on the capture, construction (i.e. use), accessibility and purpose of the information being collected and used [8]. The TL should also provide an IAS with transparent information flows, so potential and actual information flows are not obscured [41].

Bellotti observed:

> "*Whilst lack of feedback already causes problems in non-explicitly collaborative computing contexts, it is far more serious for CSCW and CMC*[7]*. As such systems increasingly support information sharing and communication, it is important for people to understand when they and their information are accessible, when, and to whom."* [7]

A practical example of providing users with an accurate view of information use in a collaborative computing context is the prototype file-sharing manager of Whalen *et al.* [74], which dynamically informs users of the files currently being shared within a collaborative workspace.

6. TRUST AND THE PST FRAMEWORK

Having examined the privacy layers in an IAH and a TL, it is instructive to consider how the PST Framework can be used to assist practitioners in understanding how activities at each layer contribute to the construction of trust between trustor and trustee. Camp *et al.* suggest that "*trust is necessary and extant on the Internet*" on three levels: 1) "*the nuts and bolts level of the router system*"; 2) "*other people will behave in ways that uphold the community norms"*; and 3) "*institutions – such as Internet businesses - will conduct themselves in ways that are conducive to productive ongoing transactions*" [12], hinting at the appositeness of a layered approach to the construction of trust. Riegelsberger *et al.*'s [56] trust framework can be used to understand how activities at each layer contribute to overall trust between an IAS and an IAR.

One of the intrinsic properties of a trustee that engenders trust in a trustor is *ability* i.e. "[…] *whether an actor is able to fulfill* [what is requested of them]" [56], which includes factors such as professionalism and domain-specific expertise; similar to Camp's idea of *competence* as a component of *operational trust* [11]. Ability (or competence) also applies to technical trustees and includes the following dimensions: confidentiality, integrity, authentication, non-repudiation, access-control, error rates and availability [56] - dimensions which neatly fall into the Information Security Layer. Ability must therefore be expanded to include the ability of technology service to safeguard its IAs. As one respondent in Bamberger & Mulligan's study observed, the ability to "*deliver those consistent experiences, compliant experiences, you know, that's trust*" [6].

The other two intrinsic properties of a trustee are *internalized norms* (e.g. honesty, credibility, reliability, dependability, good morals, goodwill, openness etc.) and *benevolence* (e.g. good corporate citizenship, exceeding customers' expectations, good intentions etc) [56], encapsulated in Camp's idea of *intent* as a component of *operational trust* [11]. Both of these properties are likely to be significantly influenced by organizational culture and ethics, and hence will also affect the Information Privacy Culture Layer – if an organization has generally good morals it is likely to have a similarly good information culture and information ethics. The intrinsic properties of a trustee identified can be mapped to the privacy layers in an IAR (Table 2); note how the Information Principles Layer is split between *ability* and *internalized norms and benevolence.*

Table 2. Mapping between the Trust Framework of Riegelsberger *et al.* and IAR Information Privacy Layers

Intrinsic Property of Trustee	IAR Information Privacy Layer
Ability	• *Information Security Layer* – ability to protect IAs. • *Information Management Layer* – ability to manage IAs effectively. • *Information Principles Layer* – Adherence to relevant data protection legislation where available ('letter of the law').
Internalized Norms and Benevolence	• *Information Principles Layer* – Principles governing information use which exceed legislative requirements (e.g. 'company law' [6]), which aim to respect consumers' information and their privacy expectations ('spirit of the law'). • *Information Use Layer* – Information use, notification and consent, which exceeds the safeguards set out in fair information practices. • *Information Privacy Culture Layer* – Actual use of information is as expected by the trustor.

An example of privacy being only one dimension of ability is a scenario in which an IAS (e-commerce customer) browses an IAR's (vendor's) web site for products, trusting their *ability* to deliver a quality product as requested, but not comfortable to trust their *ability* to maintain the IAS's privacy. This may be because of the IAS's mistrust in the IAR's privacy practice and/or TL (web site). In the former case, the consumer may telephone the vendor with their credit card and address details, in the latter case they may send a check, or pay with cash.

The IAR, through the technology service and other channels (e.g. advertising, brand awareness etc.), must make its privacy practice visible to the IAS. This is achieved through trust symbols, and visibility of trust symptoms [56] at each layer of the PST Framework. For example, the use of the trust symbol HTTPS may lead an IAS to trust a technology service at the Information Security Layer, but not at the Information Principles Layer due to an unclear privacy policy, or the trust symptom of poor feedback on a review web site regarding the use of IAs by the IAR for targeted marketing. The overall trust between the IAS and a technology service is therefore a function of the trust at each of the layers. Table 3 provides examples of the trust signals provided by a technology service at each layer.

Schneier [57] suggests there are four societal pressures: 1) moral pressure; 2) reputational pressure; 3) institutional pressure; and 4) security systems (i.e. defenses and detection systems), which make it more difficult and less attractive – in terms of consequences - for a trustee in a transaction to defect and serve its own self-interest. The existence of these pressures assists a trustor in making a risk trade-off when deciding whether to trust a trustee. As shown in Table 4, these societal pressures are likely to influence an IAR's privacy practice activities, and can therefore be mapped to four of the layers in the PST framework.

[7] Computer-supported collaborative work and computer-mediated communication respectively.

Table 3. Examples of Trust Signals at each Information Privacy Layer in an IAR and TL

Information Privacy Layer	Example of Technology Service's Trust Signals
Information Privacy Culture	An IAR's privacy decision making concerning IAs entrusted to it - directly or vicariously experienced by an IAS. For example an IAR who is known for passing IAs entrusted to it to other IARs for its own financial gain will suffer a reduction in trust.
Information Use	The clarity and transparency of an IAR's statement of *intended information use*, e.g. its privacy policy (although users have a reluctance to read privacy policies [72]). The degree of alignment between *expected information use* and *experienced information use*.
Information Principles	The statements set out in a technology service's privacy policy.
Information Management	The ability of a technology service to provide technology and processes for an IAS to exercise control over the IAs it has entrusted to the technology service.
Information Security	Use of technical and operational security controls to secure IAs, e.g. the use of HTTPS on a web site, user authentication, secure document storage etc.

Table 4. Mapping between Schneier's societal pressures [57] and IAR Information Privacy Layers

Societal Pressure	IAR Information Privacy Layer	Example of good privacy behavior
Moral	Information Privacy Culture Layer	It feels wrong for the organization to cheat its customers.
Reputational	Information Principles Layer ('spirit of the law')	The organization has a reputation for not passing customers' information to third-parties without their permission.
Institutional	Information Principles Layer ('letter of the law')	The organization abides by applicable data protection and privacy regulations and rules to avoid sanctions.
Security Systems	Information Security Layer	The organization's systems create audit trails of its activities, which are available to external auditors.

Although the Information Use Layer is omitted from Table 4, all four societal pressures will directly influence an organization's information use. For example, moral, reputational and institutional pressure, and security systems are all likely to prevent an organization from using its customers' sensitive personal data for social sorting or marketing purposes.

7. APPLYING THE PST FRAMEWORK

To provide a proof-of-concept application of the PST Framework, we use it to show how potential privacy problems can be identified for a new technology: smart metering. This section concentrates on the privacy issues arising from the collection of detailed electricity consumption information from smart meters, and its transmission across the smart grid. A concise definition of smart grid is that it "[...] *uses intelligent transmission and distribution networks to deliver electricity.*" [37]. Smart grids contain multiple networks: distribution, transmission, energy trading, load monitoring, substation, premises, operations and monitoring.

Existing electricity meters typically have more than one tariff (e.g. in the UK meters usually have a day and night tariff), measure total use for a household, and are usually read by a human operator visiting customers' homes quarterly. Smart meters automatically take readings at finer time intervals (e.g. every half hour), automatically transmitting them to an energy company via a smart grid.

This section assumes the IAS in the PST Framework is a household, the energy company an IAR, and the smart meter and energy consumption network within the smart grid a TL. To keep this example concise, this section will consider only the IAR and TL components of the PST Framework.

Quinn [54] has discussed many of the privacy issues arising from smart metering, but these have not been set within a framework. The purpose of this section is not to uncover new privacy issues, but illustrate how the PST Framework can be used to highlight potential shortcomings in the information privacy practices of energy companies, identifying potential weaknesses and where technology management effort should be concentrated.

7.1 Smart Metering

7.1.1 Privacy Concerns of Technology

Smart grids and the associated smart metering, although strongly encouraged by US and European governments since 2007, have led to concerns about peoples' security and privacy [4]. Furthermore, a UK pilot found no statistically significant cost savings [quoted in 4]. A high-level Privacy Impact Assessment (PIA) in 2009 highlighted a significant number of shortcomings in current attempts to address the privacy issues raised by smart meters [quoted in 17]. In 2009, the Dutch Senate rejected a Smart Metering Bill as a violation of the right to privacy under the European Convention on Human Rights [66].

The privacy implications of fine-grained meter reading have already been highlighted **[47]**: there is the potential for side-channel leakage of detailed information of a household's activities, using techniques such as Non-Intrusive Load Monitoring (NILM) systems and algorithms **[49]**. The level of information that can be determined is related to the meter reading frequency, with major appliances identifiable when meter reading takes place every minute **[47]**. A recent study demonstrated how residents' presence and sleep cycles could be estimated with high confidence using relatively unsophisticated monitoring equipment and algorithms **[42]**.

Most of the discussions regarding the privacy implications of smart meters focus on protecting the privacy of a household from the outside world. However, there are also concerns about the privacy of a household's individual members, i.e. from each other [47].

There are two paradigms for smart metering [4], each with different privacy implications: 1) local feedback or decentralized in which the meter performs data processing of fine grained readings and passes measurements to the energy company at a coarser interval, e.g. once a day or once a month; 2) remote feedback or centralized in which the meter sends detailed consumption information to the energy company. In the former case, energy use management is carried out manually, or provided within the household by a separate system. In the latter case, the energy company provides a web interface for the consumer to manage energy use [4]; local feedback is the preferred approach for the UK [26].

7.1.2 Information Asset Receiver (IAR)

7.1.2.1 Information Security Layer

If a remote feedback or centralized paradigm is used, an IAR will become responsible for a vast quantity of sensitive information assets. Initial estimates for the 47 million meters in the UK suggest data volumes of around 9Pb per year, assuming half hourly readings [4]. But there has been little information security research on the potential vulnerabilities, threats and risks of managing the real-time IAs, possibly because the assumption is that existing information security provisions will suffice. A supervisory system will be required to efficiently process vast quantities of data, allowing the energy company to monitor the smart grid and detect security or system failures [37]

Quinn [54] refers to the need for "*technological protections*" to protect data, which is the traditional paradigm for information security. Given the sensitivity around smart metering and the need to engender consumer trust in the rollout, the PST Framework should be used to correctly align information security processes with the requirements of the other layers. For example, IARs must ensure activities at this layer are part of an organizational information security culture to prevent human violations of security policy, such as copying sensitive consumer information to external media. Information handling processes must be closely examined for vulnerabilities, and technical or operational solutions designed to counter potential threats unique to smart metering.

IARs should also not be overly optimistic concerning potential security risks and should ensure their organizational culture plans for failure; working with smart meter vendors to develop recovery strategies [46].

7.1.2.2 Information Management Layer

Information management can be split into that used by an IAR to manage its information assets, and that provided via the TL to allow an IAS to control the flow of their information assets to the IAR.

With centralized smart metering in particular, an IAR will be responsible for a vast quantity of information assets, and it will therefore be imperative that rigorous processes are put in place for information lifecycle management, from collection of information from smart meters, to the organizing, processing, dissemination and deletion of that information.

As well as managing its own information assets, an IAR's information management processes should also provide an IAS with the ability to control its own information flows. Quinn [54] suggests two approaches to providing users with the ability to control information. The first is a hierarchical opt-in/opt-out regime, with a coarse-grained default opt-out as suggested by [41]; this may cause a rise in the energy rate charged due to lack of real-time energy information. The second option is to impose a privacy tariff wherein customers pay a premium to protect their privacy. Once IARs have determined their business strategy, they must ensure this flows correctly down to this layer and seamlessly through to the TL.

7.1.2.3 Information Principles Layer

Concerns were raised in 2009 about the lack of formal privacy policies, standards or procedures – what Quinn [54] calls *"procedural best practices"* - for smart metering [17]. Such policies should be placed at this layer, and represent a bare minimum of adherence – energy companies should seek to better these to gain consumer confidence and gain a competitive edge.

In the UK, DECC's response to the UK Government's Smart Metering Programme suggests energy companies obtain explicit consent for any access to personal data over and above that "[…] *required to fulfill regulatory duties."* [26] Therefore *regulatory duties* will need careful definition, with a mechanism for changing this definition when legitimately required [26]. It is likely that such regulatory duties will relate to distribution system operation, billing and planning, whose use of personal data can be minimized or avoided [4, 47]. The information principles at this layer will therefore need to be built around the agreed definition of *regulatory duties,* aim for data minimization, and protect the privacy of individual members of a household, not just the whole household [35].

7.1.2.4 Information Use Layer

Quinn [54] provides a summary of potential uses of smart meter information, categorizing them as utility services (e.g. the energy company), edge services (e.g. services provided to the consumer), or other uses (e.g. insurance adjustment and marketing). There is therefore the potential for commercial exploitation, or social sorting, through the use of data mining techniques on households' consumption patterns [17]. For example, the final privacy policy for Google's PowerMeter service has yet to be defined, allowing it to use information on households' electricity consumption for marketing purposes [46].

Given the potential for profiling individuals and repurposing of consumption information, IARs will need to provide an explicit definition of the intended and actual use of consumption information from smart meters, founded on regulatory and corporate information principles set out in the Information Principles Layer.

7.1.2.5 Information Privacy Culture Layer

The advent of smart metering means the culture of energy companies must shift from one chiefly focused on maintaining the availability of energy supplies, to one which includes safeguarding consumers' privacy.

The requirement for energy companies to have an information security culture will also be greater than ever, given the extensive regulation and governance requirements, and the complexity of the smart grid and the associated vulnerabilities caused by human agency and processes. Energy companies must have an information security culture that is sufficiently open to allow greater collaboration between academia, industry and government in evaluating smart grid security mechanisms [5, 46].

Finally, as if to stress the importance of an ethical approach to smart meter information use, a 2009 report[8] by the World Economic Forum - in partnership with Accenture – stated that "[u]*tilities, regulators and governments will need to give consumers confidence that their usage data is being handled by authorized parties in an ethical manner. Such assurances will be the key when developing the public perception of these new technologies*." [quoted in 17]

7.1.3 Technology Lens (TL)

Cavoukian [17] proposes the use of SmartPrivacy design guidelines – essentially PbD with a wider scope encompassing law, accountability, data security, fair information practices etc. – for the entire smart metering domain. This section briefly considers some of the privacy and security concerns around the smart metering TL.

7.1.3.1 Information Security Layer

Some of the security concerns of smart metering that have been raised include, consumer fraud, smart meter 'worms' [46], and the potential for damage to promulgate between transmission systems because of their interconnectedness [37].

Another major security concern is the ability to remotely switch off electricity supplies to large numbers of customers, providing an unparalleled level of vulnerability from cyber-attacks or software failures [5]. This last vulnerability is recognized by NIST in the US and Ofgem in the UK, and requires a solution at this layer using security techniques such as shared control, backup encryption keys, local override and rate-limiting mechanisms [5].

7.1.3.2 Information Management Layer

As one of the aims of smart metering is to allow customers to control their energy use, lowering overall demand and electricity costs, they will need to be provided with the ability to define and control their energy policy (e.g. by setting household devices to automatically switch on and off at user-specified times) [5]. This layer must therefore provide the user with accurate and timely tariff and consumption information, along with the potential costs and savings for switching each household appliance on or off.

This layer should also provide households with strong control over the IAs sent to the IAR [42].

7.1.3.3 Information Principles Layer

Cavoukian [17] offers a high-level set of SmartPrivacy design principles, from which the information principles at this layer could be created. Substantial engineering work is still required however to understand how these principles are implemented in the two layers below (Information Management Layer and Information Security Layer).

One possible technological approach to minimizing the data has been suggested by Lisovich *et al.* [42]; this uses protocols to carry out most of the data processing in the residence, with hard rules regarding the transmission of certain types of information.

7.1.3.4 Information Use Layer

One of the key engineering principles of PbD is data minimization [38], and one of the recommendations for smart metering design is the collection of the minimum amount of data required [17]. To simplify the problems of different information use requirements for householders and energy companies, Quinn [54] proposes bundling, so technology would need to enable the capture and use of information on the dimensions of: customer (individual to aggregated); time-shifting (real-time to delayed); and resolution (meter level to consumer level). These different bundles would be selectable by the consumer and would be an important determinant in eventual information use, along with, for example, information sharing preferences.

8. CONCLUSION AND FURTHER WORK

We have presented an integrated Privacy, Security and Trust (PST) Framework as a tool for understanding the composition of privacy for IAHs partaking in technology-mediated interactions. It offers a socio-technical approach to placing information security, privacy in technology-mediated interactions, trust, PbD guidelines, technology management processes, data protection and governance legislation, and information and security culture and ethics into a single framework.

For practitioners, the PST Framework addresses two problems: 1) it provides a clear hierarchy of the activities needed to plan, deploy and maintain privacy, from the softer organizational attributes of culture down to the pragmatic considerations of information security; and 2) it offers a framework to assist in understanding where weaknesses may be in an IAH's privacy activities. More specifically, the PST Framework: 1) clearly delineates information security from privacy; 2) integrates information security culture with privacy; and 3) places data protection at the heart of those activities involved in maintaining privacy, rather than restricting it to a function of information security.

The PST Framework should not be considered prescriptive – a single privacy practice suitable for all IAHs and all contexts is infeasible. Nevertheless, the framework provides a common reference model with a layered approach, which supports information privacy provision founded on sound information security practices and information management. The lower four layers of the PST Framework provide a structure into which an IAH can place its processes and procedures for privacy protection, to not only mitigate the risk of legislative action, but also protect IASs from substantive harms to their privacy.

The PST Framework also helps an IAH to:

- determine if the services provided at each layer are sufficiently rich; and
- check the existence of a logical privacy hierarchy flowing from top to bottom thus:
  - **Information Privacy Culture Layer**: A strategic view of privacy and security based on an explicit ethical position.
  - **Information Use Layer**: A clear, accurate statement of intended and advertised IA use.
  - **Information Principles Layer**: Adherence to the legislative and governance environment for IAs, as well as 'company law' [6] (where applicable).
  - **Information Management Layer**: Processes, policies and technical mechanisms used for IA management, which provide accurate and timely actual IA use.

[8] *Accelerating Smart Grid Investments*.

- **Information Security Layer**: The technical and physical controls to ensure security of IAs against identified threats.

The PST Framework could also provide a basis for the development of a two-dimensional Capability Maturity Model [52] for privacy, in which privacy provision in each layer not only passes through the steps of *Initial*, *Repeatable*, *Defined*, *Managed* and *Optimizing*, but the addition of each layer, from the Information Security Layer above, provides evidence of increasing privacy maturity, until an ideal IAH in which all layers exist, operating at the *Optimizing* level.

The ability to measure the maturity of an IAR's privacy practice at each layer of the PST Framework, and trace its privacy activities through its technology platform, may provide a useful basis for structuring audits – particularly Privacy Impact Assessments (PIA) – of IAR's actual information privacy practices. A PIA could be structured to ensure each layer is the correct refinement of the layer above.

One of the possible criticisms of the PST Framework is that a layered paradigm is too simplistic, resulting in an IAH creating a set of disconnected 'islands of responsibility' at each layer, with their boundaries becoming points of weakness. A partially ordered set may therefore be a more accurate representation of the functional dependencies among the people, processes and technology required for effective privacy practice. However, the PST Framework – in common with many frameworks - is a simplified and abstracted view of reality, yet sufficient to assist practitioners in reasoning about the capability of the lower layers to support the upper layers.

The OSI network model analogy used in the PST Framework could be developed further, so that each layer has a technology-agnostic interface defining the services it offers to the layer above. This would allow an IAH to determine if each layer provides a sufficiently rich set of services to support the layer above. For example, an IAH would be able to confirm that its information management (Information Management Layer) was able to support the relevant legislative data protection requirements (Information Principles Layer), such as the ability to quickly locate all copies of an IA relating to a subject access request, or to locate and delete all copies of an IA.

With the concept of a TL, the PST Framework also allows tracing of links between the privacy activities of an IAR and the design of a TL. Using the PST Framework, an IAR can determine if their information principles are correctly instantiated in the TL, and that the information management mechanisms within its user interface (e.g. the ability to opt-in/opt-out, and the feedback and control provided by the Information Management Layer) can be supported by the services offered by the IAR's Information Management Layer. It is hoped such an approach will help to avoid situations wherein the sound privacy practices of an IAR are distorted by a poorly designed or implemented TL. Work in formalizing HIPAA legislation using Prolog to check the compliance of a simple web-based messaging system [39] could offer a useful possible approach to check the correctness of each layer's implementation in the IAR and associated TL.

This paper has described several new constructs within the PST Framework:

- **Technology lens**: A layered view of the privacy characteristics of a technology linked to PbD principles.
- **Technology service**: A socio-technical system formed from an IAR and TL.
- **Information privacy culture**: Formed from the intersection of an IAH's information culture, information security culture, and information ethics.

Development of the PST Framework is at an early stage, and there remains much work to complete. This paper has shown it to be a valuable tool - particularly for practitioners - to provide a roadmap to maintaining privacy. Indeed, the PST Framework can be used by organizations to define what "*a wonderful privacy program means*" [6].

Our title for this paper is "*Privacy is a Process, not a PET*", because if the PST Framework is used to help in implementing effective privacy practice in organizations - seamlessly linking it to a technology lens designed according to PbD principles – there should be less need for PETS.

9. ACKNOWLEDGMENTS

With thanks to Anthony Morton's secondary doctoral supervisor, Gus Hosein, for his suggested addition of the concept of a technology lens to the PST Framework. Thanks also to the NSPW '12 attendees and anonymous reviewers who provided constructive comments and suggestions to help improve this paper. Particular thanks are owed to Susan Landau who shepherded this paper through NSPW '12. Anthony Morton is funded by a PhD scholarship - part of a UK Engineering and Physical Sciences Research Council (EPSRC) grant (EP/G034303/1) - from the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast.

10. REFERENCES

[1] Adams, A. 2001. *Users' Perceptions of Privacy in Multimedia Communications*. Unpublished PhD Thesis, School of Psychology, University College London.

[2] Adams, A. and Sasse, M.A. 2001. Privacy in Multimedia Communications: Protecting Users, Not Just Data. *Human-Computer Interaction* (2001).

[3] Adams, A. and Sasse, M.A. 1999. Privacy Issues in Ubiquitous Multimedia Environments: Wake sleeping dogs, or let them lie? *IFIP Conference on Human-Computer Interaction* (1999).

[4] Anderson, R. and Fuloria, S. 2010. On the security economics of electricity metering. *The Ninth Workshop on the Economics of Information Security* (2010).

[5] Anderson, R. and Fuloria, S. 2010. Who controls the off switch? *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* (2010), 96–101.

[6] Bamberger, K. and Mulligan, D. 2010. Privacy on the Books and on the Ground. (2010).

[7] Bellotti, V. 1996. What You Don't Know Can Hurt You: Privacy in Collaborative Computing. *Proceedings of HCI on People and Computers XI* (London, UK, 1996), 241–261.

[8] Bellotti, V. and Sellen, A. 1993. Design for Privacy in Ubiquitous Computing Environments. (1993).

[9] Berti, J. 2003. Social engineering: The forgotten risk. *Canadian HR Reporter*. 16, 13 (Jul. 2003), 21,23.

[10] Boyce, G. 2002. Beyond privacy: the ethics of customer information systems. *Informing Science*. (2002), 107–125.

[11] Camp, L. 2003. Designing for Trust. *Trust, Reputation, and Security: Theories and Practice*. (2003), 203–209.

[12] Camp, L. et al. 2002. Trust: A Collision of Paradigms. *Financial Cryptography* (2002), 91–105.

[13] Camp, L.J. 2001. *Trust and risk in Internet commerce*. The MIT press.

[14] Cavoukian, A. 2009. *Privacy by Design*. Office of the Information and Privacy Commissioner.

[15] Cavoukian, A. 2011. *Privacy by Design - The 7 Foundational Principles*. Office of the Information and Privacy Commissioner.

[16] Cavoukian, A. 2009. *Privacy by Design ... Take the Challenge*. Office of the Information and Privacy Commissioner. Ontario.

[17] Cavoukian, A. et al. 2010. Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*. 3, 2 (2010), 275–294.

[18] Cavoukian, A. 2009. SmartPrivacy: Lead with Privacy by Design.

[19] Chan, Y.E. and Greenaway, K.E. 2005. Theoretical Explanations for Firms' Information Privacy Behaviors. *Journal of the Association for Information Systems*. 6, 6 (Jun. 2005).

[20] Choo, C.W. et al. 2008. Information culture and information use: An exploratory study of three organizations. *Journal of the American Society for Information Science and Technology*. 59, 5 (Mar. 2008), 792–804.

[21] Choo, C.W. et al. 2006. Working with information: information management and culture in a professional services organization. *Journal of Information Science*. 32, 6 (Dec. 2006), 491 –510.

[22] Culnan, M.J. and Williams, C.C. 2009. How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. *MIS Quarterly: Management Information Systems*. 33, 4 (2009), 673–687.

[23] Curry, A. and Moore, C. 2003. Assessing information culture—an exploratory model. *International Journal of Information Management*. 23, 2 (Apr. 2003), 91–110.

[24] Davenport, T.H. and Prusak, L. 1997. *Information ecology: Mastering the information and knowledge environment*. Oxford University Press, USA.

[25] DeCew, J.W. 1997. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Cornell University Press.

[26] Department of Energy and Climate Change 2011. *Smart Metering Implementation Programme: Response to Prospectus Consultation. Supporting DOcument 1 of 5 - Data Access and Privacy*. Department of Energy and Climate Change - Smart MeteringTeam.

[27] Dhillon, G. 2001. Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*. 20, 2 (2001), 165–172.

[28] European Commission 2010. *A comprehensive approach on personal data protection in the European Union*. Technical Report #COM(2010) 609 final.

[29] European Parliament & Council 1995. *The protection of individuals with regard to the processing of personal data and on the free movement of such data*.

[30] Federal Trade Commission 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace - A Report to Congress*.

[31] Gefen, D. et al. 2003. Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*. 27, 1 (2003), pp. 51–90.

[32] Gelman, R. 2012. Fair Information Practices: A Basic History.

[33] Good, N.S. and Krekelberg, A. 2003. Usability and privacy: a study of Kazaa P2P file-sharing. *Proceedings of the SIGCHI conference on Human factors in computing systems* (New York, NY, USA, 2003), 137–144.

[34] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: 1980. *http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*. Accessed: 2012-10-26.

[35] Gürses, S. et al. 2011. Engineering privacy by design. *Computers, Privacy & Data Protection*. (2011).

[36] ISO/IEC 27000 Series 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[37] Khurana, H. et al. 2010. Smart-Grid Security Issues. *IEEE Security & Privacy*. 8, 1 (Feb. 2010), 81–85.

[38] Kung, A. et al. 2011. Privacy-by-design in ITS applications. (Jun. 2011), 1–6.

[39] Lam, P. et al. 2009. A Formalization of HIPAA for a Medical Messaging System. *Trust, Privacy and Security in Digital Business*. S. Fischer-Hübner et al., eds. Springer Berlin / Heidelberg. 73–85.

[40] Langheinrich, M. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. *Ubicomp 2001: Ubiquitous Computing* (2001), 273–291.

[41] Lederer, S. et al. 2004. Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing*. 8, 6 (2004), 440–454.

[42] Lisovich, M. and Wicker, S. 2008. Privacy concerns in upcoming residential and commercial demand-response systems. *Proc. of the Clemson University Power Systems Conference (Clemson, SC, March, 2008)*. (Mar. 2008).

[43] Martins, A. and Eloff, J.H.P. 2002. Information security culture. *Security in the Information Society*. (2002), 203–214.

[44] Mason, R.O. 1995. Applying ethics to information technology issues. *Commun. ACM*. 38, 12 (Dec. 1995), 55–57.

[45] Mason, R.O. et al. 1995. *Ethics of Information Management*. Sage Publications, Inc.

[46] McDaniel, P. and McLaughlin, S. 2009. Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy*. 7, 3 (Jun. 2009), 75–77.

[47] McKenna, E. et al. 2012. Smart meter data: Balancing consumer privacy concerns with legitimate applications. *Energy Policy*. 41, (Feb. 2012), 807–814.

[48] McKnight, D.H. and Chervany, N.L. 2001. What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *International Journal of Electronic Commerce*. 6, 2 (2001), 35–59.

[49] Molina-Markham, A. et al. 2010. Private memoirs of a smart meter. *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (New York, NY, USA, 2010), 61–66.

[50] Nissenbaum, H. 2004. Privacy as contextual integrity. *Washington Law Review*. 79, (2004), 119.

[51] Oxford English Dictionary 2011. Asset. *Oxford English Dictionary (Online Version)*. Oxford University Press.

[52] Paulk, M.C. et al. 1993. *Capability Maturity Model for Software (Version 1.1)*. Technical Report #CMU/SEI-93-TR-024. Carnegie Mellon University, Software Engineering Institute.

[53] Quinn, B. and Arthur, C. 2011. PlayStation Network hackers access data of 77 million users. *The Guardian*.

[54] Quinn, E.L. 2009. *Smart Metering and Privacy: Existing Laws and Competing Policies*.

[55] Ratnasingham, P. and Pavlou, P.A. 2003. Technology Trust in Internet-Based Interorganizational Electronic Commerce. *Journal of Electronic Commerce in Organizations*. 1, 1 (2003), 17–41.

[56] Riegelsberger, J. et al. 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*. 62, 3 (2005), 381–422.

[57] Schneier, B. 2012. *Liars and Outliers: Enabling the Trust That Society Needs to Thrive*. John Wiley & Sons.

[58] Schneier, B. 2004. *Secrets and Lies: Digital Security in a Networked World*. Wiley Publishing Inc.

[59] Smith, H.J. 2002. Ethics and information systems: Resolving the quandaries. *SIGMIS Database*. 33, 3 (Aug. 2002), 8–22.

[60] Smith, H.J. 1993. Privacy Policies and Practices: Inside the Organizational Maze. *Communications of the ACM*. 36, 12 (1993), 104–122.

[61] Smith, H.J. and Hasnas, J. 1999. Ethics and Information Systems: The Corporate Domain. *MIS Quarterly*. 23, 1 (1999), pp. 109–127.

[62] Solove, D. 2009. *Understanding Privacy*. Harvard University Press.

[63] Spy law "used in dog fouling war:" 2008. *http://news.bbc.co.uk/1/hi/uk/7369543.stm*. Accessed: 2012-10-29.

[64] Sydnor, T.D. et al. 2006. *Filesharing Programs and "Technological Features to Induce Users to Share."* United States Patent and Trademark Office.

[65] Thomson, K.-L. et al. 2006. Cultivating an Organizational Information Security Culture. *Computer Fraud & Security*. 2006, 10 (Oct. 2006), 7–11.

[66] Tilburg University 2009. Dutch Senate rejects Smart Metering Bill.

[67] Timeline: Child benefits records loss: 2008. *http://news.bbc.co.uk/1/hi/7104368.stm*. Accessed: 2012-10-29.

[68] U.K. Information Commissioner's Office 2008. *Privacy by Design*. U.K. Information Commissioner's Office.

[69] U.S. Department of Homeland Security 2008. *Privacy Policy Guidance Memorandum*.

[70] Da Veiga, A. and Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. *Computers & Security*. 29, 2 (Mar. 2010), 196–207.

[71] Veiga, A.D. and Eloff, J.H.P. 2007. An Information Security Governance Framework. *Information Systems Management*. 24, (Oct. 2007), 361–372.

[72] Vila, T. et al. 2003. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. *Proceedings of the 5th international conference on Electronic commerce*. (2003), 403–407.

[73] Westin, A.F. 1967. *Privacy and Freedom*. Atheneum.

[74] Whalen, T. et al. 2008. Information displays for managing shared files. *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology* (2008), 1–10.

[75] Wiedmann, K.-P. et al. 2010. Determinants of Consumers' Perceived Trust in IT-Ecosystems. *Journal of theoretical and applied electronic commerce research*. 5, 2 (Aug. 2010), 137–154.