PS4TLA: Privacy Support for the Total Learning Architecture

Specification Document, version 0.1:

Operational Characteristics

Author information

Project lead: Dr. Bart P. Knijnenburg, Clemson University

Project team: David Cherry, Daricia Wilkinson, Saadhika Sivakumar, Reza Ghaiumy Anaraky, Moses Namara, Dr. Erin Ash, Rosey Davis

Technical point of contact: Dr. Elaine Raybourn, Sandia National Laboratories

Executive summary

The purpose of this document is to inform ADL and other TLA performers about the Operational Characteristics that impact users’ privacy concerns and to make recommendations for implementing a Privacy by Design (PbD) model where privacy decisions of the system are made in its initial developmental stages. The set of recommendations put forth in this document will allow ADL and other TLA performers to select the characteristics that best alleviate users’ concerns.

In the first section, User Characteristics, the variance in individuals’ privacy concerns are considered. Personal characteristics of users, including decision-making mechanisms, cognitive-processing practices, and communication styles, have significant implications for their privacy management behaviors. To address these characteristics, it is recommended that TLA tailor to different privacy management strategies and communication styles in its design. For example, users should be given options for selective sharing of their information and outcomes, and both social-network style and direct, chat-style interaction features should be available.

A section on Input Data Characteristics addresses issues surrounding the collection of users’ personal information. Data collection is fundamental to providing personalized learning experiences that adapt to users. However, it is important to consider the privacy implications of collecting the potentially sensitive data about users that is necessary for adaptive systems to function effectively. In some cases, the TLA may make incorrect predictions or predictions that users may be uncomfortable with. To solve this issue, users should be allowed to scrutinize and correct potential mistakes in system predictions, as well as to venture beyond the personalized recommendations.

The Output Characteristics section offers recommendations for presenting adaptations to users. Personalized notifications are an important feature of the TLA architecture, which specifies three types of adaptations, specifically providing individualized recommendations to switch from one Learner Activity to another, determining the next learning activity within a single activity provider, and adapting learning content within a single learning activity. For these mechanisms to be effective, they must be accurate without being intrusive or inconvenient. Notifications should be carefully planned to prevent interrupting a user’s current task. Systems should also be designed to prevent leaking personal information in social settings by providing only generic notifications or, where possible, tailoring notifications to specific social settings.

A section titled Data Location and Ownership addresses questions of data location and ownership from a user-privacy perspective. Because the TLA is inherently decentralized by design, it is important decisions about where collected data will be stored and what entities have access to it must be made. Such decisions should reflect the spirit of “open” learning models by giving users ownership over their data. Of course, employers and apps will necessarily have access to some data, but access should be limited to narrowly specified purposes and take steps
to maintain user privacy, such as de-identifying data when possible. Another strategy may be to allow users to designate a “data steward” to manage their data in accordance with their privacy preferences. The TLA should also make user models portable so users can take their data with them as they move between employers.

The **Data Sharing** section outlines how recipients of user data can preserve user privacy when using the data for various purposes. It is important for managers to communicate secondary data usage practices to users; users should be aware of what information collected about them is used and how. Managers should also act responsibly regarding placement and promotion decisions by being transparent about the guidelines they use to assess potential conflicts between competencies and preferences and to prevent discriminatory practices. Finally, Institutional Research Board (IRB) guidelines for research, which require data to be anonymized to the degree possible, should be followed.

The last section, **Privacy Support Mechanisms**, discusses techniques for user-tailored privacy (UTP). UTP moves beyond a “one-size-fits-all” approach to privacy design by accounting for the high variability and context-dependency of people’s privacy decisions. UTP aims to strike a balance between giving users no control over their privacy, which may elicit privacy concerns, and giving users full control over their privacy, which is often unmanageably complex for the typical user. Successful implementation of UTP requires taking such steps as using accessible privacy controls, and using users’ behavioral patterns to make privacy-related adaptations.

Given the complexity of privacy in advanced distributed learning systems, upcoming versions of this document will delve deeper into the idea of user-tailored privacy as a decision-support mechanism for TLA. For the final document, we will seek consensus among TLA performers regarding the operational characteristics and the implementation of user-tailored privacy. This will allow us to make specific and concrete recommendations regarding privacy support for TLA.
Introduction

Purpose

The Total Learning Architecture (TLA) is a set of specifications to enable the development of next-generation learning systems. As the TLA specifications are being developed, there exists an opportunity to implement Privacy by Design (PbD), where privacy is treated as a fundamental part of the system, and taken into account throughout the entire development lifecycle of the system, starting at the early stages of design and development [51, 207, 308, 314, 335]. This document therefore describes the potential impact of the Operational Characteristics (OCs) of TLA-based systems on users’ privacy concerns. The OCs are aspects of TLA-based systems that can be implemented in various ways. The purpose of this document is to allow ADL and other TLA performers to select the operational variants that best alleviate users’ privacy concerns.

Scope

This document describes the operational variations of privacy-relevant OCs of distributed learning systems in general—and specifically of TLA—as well as their impact on users’ privacy concerns. Where possible, an attempt is made to juxtapose the privacy concerns with the benefit of the described operational variant.

This document is written to support both the current development of the TLA specifications, as well as current and future implementations of these specifications in real-life distributed learning systems. The described OCs and their variants may therefore go beyond any currently envisioned specification and implementation of TLA.

OCs that are not privacy-relevant are not discussed in this document. Most notably, this document does not concern the security of the TLA. Security-related OCs are only discussed where they intersect with user privacy concerns.

Several types of actors are involved in the development of the TLA specifications, and the implementation and operation of distributed learning systems based on these specifications. To aid different actors in navigating this document, we highlight parts of it that are particularly relevant for specific audiences. These audiences are described in Table 1.

Where possible, the document contains concrete recommendations. Further recommendations will be added after intensive discussion with ADL and other TLA performers during the development of version 1.0 of this document.
Table 1: Actors that form the potential audiences for this document.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="training_manager.png" alt="Icon" /></td>
<td><strong>Training Manager</strong>—Responsible for evaluation, promotion, mission planning, user data management and research</td>
</tr>
<tr>
<td><img src="activity_developer.png" alt="Icon" /></td>
<td><strong>Activity Developer</strong>—TLA End User Application Developers who develop and implement the TLA user facing apps</td>
</tr>
<tr>
<td><img src="backend_developer.png" alt="Icon" /></td>
<td><strong>TLA Backend Developer</strong>—Develops the Data Core and TLA Processors</td>
</tr>
<tr>
<td><img src="applicable.png" alt="Icon" /></td>
<td>Applicable to Training Manager + Activity Developer</td>
</tr>
<tr>
<td><img src="applicable.png" alt="Icon" /></td>
<td>Applicable to Activity Developer + TLA Backend Developer</td>
</tr>
<tr>
<td><img src="applicable.png" alt="Icon" /></td>
<td>Applicable to all</td>
</tr>
</tbody>
</table>

Definitions and Abbreviations

The **Total Learning Architecture (TLA)** is a set of specifications to enable the creation of a next-generation Learning Management System (LMS). These specifications consist of a set of web service specifications and APIs for sharing learning-related user data in a consistent way, thereby allowing the integration of learning applications (User Facing Apps created by Activity Providers) ranging from eBooks to Massively Open Online Courses (MOOCs) into comprehensive personalized e-learning solutions [310]. The TLA specifies ubiquitous data collection (e.g. by integrating a wide variety of learning applications, interfacing with social media activity, and tracking smartphone sensors) and user modeling (e.g. by collecting highly detailed learner runtime activity) to enable highly personalized and pervasive (On The Job, Just In Time) training recommendations, calculated by the TLA Providers [98]. Moreover, the TLA specifications calls for an Open Social Learner Model (OSLM) that allows learning materials, activities, and outcomes to be shared across learners (enabling peer interactions) and learning systems (allowing for an extensible learning environment) [370]. This document describes how certain characteristics of
the TLA specification—and of distributed learning systems implementing these specifications—have an impact on users’ privacy concerns.

**Privacy by Design (PbD)** is a design philosophy in which privacy aspects are addressed early in the system design and development process, rather than after the system has been developed ("post hoc privacy") [51, 207, 308, 314, 335]. While post hoc privacy solutions typically try to mitigate privacy problems that exist within a system, PbD tries to avoid privacy problems from occurring at all. This document addresses PbD by analyzing the proposed operational characteristics of the TLA from a privacy perspective.

An **Operational Characteristic (OC)** is an aspect of TLA that influences the users’ experience. OCs are compositional, in that each OC (e.g. “input data”) consists of underlying sub-OCs (e.g. “learner runtime activity”, “smartphone tracking data”). An OC can be implemented in multiple ways across different operational dimensions (e.g. learner runtime activity may be tracked in a “granular” or “aggregated” manner, either in “real time” or “asynchronous”)—these are called operational variants. A privacy-relevant OC is defined as an OC whose variants have an impact on users’ privacy concerns.

**Personally Identifiable Information (PII)** is information that reveals a person’s real-life identity, e.g. their name, social security number, or (in most cases) their primary email address.

**De-identification** is the practice of removing Personally Identifiable Information (PII) from a set of data. Given that data that are in themselves not personally identifiable may be designated as PII when used in combination, the term *k*-anonymity is used to characterize a dataset as containing no less than *k* exemplars of a certain combination of values. Generally speaking, a dataset is considered de-identified when all PII is removed, and *k*-anonymity is guaranteed for all combinations of non-PII data.

**Pseudonymity** is a means to identify a person in a system without revealing any links to their true identity outside the system. Pseudonymity is usually implemented by allowing users to choose a username that deviates from their real name.

The **Health Insurance Portability and Accountability Act (HIPAA)** establishes data privacy and security provisions for safeguarding medical information.

**Overview**

Privacy threats have shown to be an important barrier to the adoption of personalized systems [21, 54, 105, 193, 289, 317, 342, 357, 366], and it is therefore of utmost importance that such threats are minimized in any TLA-based system. From a privacy perspective, the social capital-based advantages of freely sharing learner profiles are at odds with the fact that these learner profiles may be protected by laws like FERPA, since these profiles are also used for sensitive employment decisions regarding placement, selection and promotion. On top of this, the envisioned international deployment of TLA introduces prominent cultural variation in privacy
concerns and social etiquette [48, 59, 68, 79, 209]. Because of this, users of TLA-based distributed learning systems must carefully navigate a multi-dimensional array of privacy concerns, carefully balancing the benefits and risks of disclosing or allowing access to their personal information. However, users of complex information systems have been consistently incapable of effectively managing their own privacy [7, 155, 157, 185, 205, 225, 231], leaving them vulnerable to perceived and real privacy threats.

Fortunately, the TLA specifications and reference implementation are still in the early stage of development, which presents an opportunity to implement Privacy by Design (PbD). This document supports a comprehensive implementation of PbD by systematically investigating the impact of the Operational Characteristics (OCs) of TLA-based distributed learning systems on users’ privacy. This allows ADL and other TLA performers to make informed decisions about which operational variations present the optimal tradeoff between privacy and other considerations. In cases where less-than-ideal privacy solution may be preferred for other reasons, the specification suggests mitigating (post hoc) solutions to limit the impact on users’ privacy.

This document considers the following OCs and sub-OCs:

1. **User characteristics**¹ (learners’ privacy decision-making practices)
   1.1. Decision-making
   1.2. Elaboration likelihood
   1.3. Communication style
2. **Input data characteristics** (data collection by the TLA Data Core)
   2.1. Levels of identifiability
   2.2. Collection of various data types
   2.3. Inferences made based on collected data
3. **Output characteristics** (mechanisms for conveying learning adaptations to the users)
   3.1. Recommendation presentation methods and mechanisms
   3.2. Output modalities and devices
   3.3. Feedback and conversation about recommendations
4. **Data location and ownership** (learner data management within TLA-based architectures)
   4.1. Managing meta-, macro-, and micro- adaptations
   4.2. Data ownership and stewardship
5. **Data sharing** (social and organizational aspects of distributed learning systems)
   5.1. Scrutability and the quantified self
   5.2. Social learning experiences
   5.3. Assessment, promotion, and mission planning
6. **Privacy support mechanisms** (supporting learners’ privacy decision-making)
   6.1. Privacy notices

¹ User characteristics are of course outside the control of the system developers, but provide important parameters that need to be considered in the design of the TLA’s privacy features.
6.2. Control mechanisms  
6.3. Privacy nudging  
6.4. User-tailored privacy

Each OC and sub-OC is further unpacked, and the tradeoff between privacy and other considerations are described for all operational variations. Where possible, concrete recommendations are made. Further recommendations will be added after intensive discussion with ADL and other TLA performers.
1 User characteristics

Problem: What is the user’s perspective? The main purpose of this document is to define operational parameters for the TLA that are acceptable for its users from a privacy perspective. How do users react to privacy-related decisions, and how does their perspective come about?

Current state of the art: Little focus on user characteristics. A lot of the existing privacy and security literature focuses on technical solutions to privacy, and often disregards the complexities of the behavior of users who operate within this technical landscape.

Solution: Study user characteristics. In this section, we acknowledge that users vary extensively in their information disclosure behavior, as evidenced by the following research:

- Recurring privacy surveys by Westin and Harris Interactive that started in the early ‘80s consistently find a substantial diversity in users’ extent of privacy concerns. They identify three types of users: fundamentalists, the unconcerned, and a pragmatic majority [130, 131, 379, 380].
- Recent research shows that users’ disclosure behavior is multi-dimensional [184], i.e., users differ not just in the amount of information that they disclose, but also in the kind of information that they are most and least likely to disclose.
- Research shows that even for the same person, the disclosure decision depends on the context in which it is made [28, 32, 64, 143, 158, 160, 214, 220, 260, 262, 266, 276, 356, 377].
- Indeed, the variability and context-dependency of privacy preferences is at the core of many privacy theories such as Altman’s privacy regulation theory [12], Nissenbaum’s contextual integrity [259, 260], and Petronio’s communication privacy management [282, 283].

This section analyzes how these differences in privacy concerns and behaviors come about, which results in important PbD recommendations for TLA-based systems. In this section, you will learn about the user characteristics that affect privacy concerns and behaviors, with specific consideration of individuals’:

- Decision-making mechanisms
- Cognitive processing practices
- Communication styles

Key findings and recommendations are presented in Table 2.
### 1.1 Decision-making

It is important to first acknowledge the mechanisms by which users make privacy-related decisions. While the benefits of adopting TLA specifications may be abundant, there are also various challenges that exist with the collection of large amounts of data. Advances in storage capabilities and data mining abilities enable the TLA Data Core to have a deeper analysis of the preferences and behavior of its users by collecting a vast amount of data [237]. This includes very detailed real-time information from users’ cellphone and other type of devices that could reveal information about the decision-making process or personal stances on sensitive topics that they normally would not share with other people or other systems.

Research shows that users acknowledge the benefit of data collection for personalization [366] but when taken too far, the same data collection can deter users from using the system extensively, or even dissuade them from using the system at all. This subsection discusses the research that quantifies this phenomenon, which has been labeled the **personalization-privacy paradox** [21, 54, 104]. We highlight the value of doing user research, building trust, and highlighting the relevance of the information that is being collected (see Table 3).

#### Table 3: Recommendations regarding decision-making

<table>
<thead>
<tr>
<th>Survey Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Perform scenario-based experiments to quantify the effects of various data collection practices</td>
</tr>
<tr>
<td>− Conduct in-depth interviews to uncover users’ privacy-related attitudes</td>
</tr>
<tr>
<td>− Perform controlled user experiments to detect potentially deleterious effects of heuristic decision practices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Build Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Ensure that the learning applications originate from trustworthy sources</td>
</tr>
<tr>
<td>− Employ sensible data collection practices and a privacy by design philosophy from the outset</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Highlight Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Highlight the potential improvements in content relevance, time saving, enjoyment and novelty</td>
</tr>
<tr>
<td>− Refrain from asking for information in situations in which the relevance is not readily apparent</td>
</tr>
</tbody>
</table>
Starting with the basic research on information disclosure, one of the most-used (cf. [223, 280, 325]) conceptualizations of users’ conscious process behind their information disclosure decisions is the “privacy calculus” [211, 212]. This conceptualization has been used by many researchers to investigate the antecedents of information disclosure [69, 70, 80, 128, 170, 220, 246, 281, 386, 394, 396].

The privacy calculus is a privacy-specific instance general human decision-making theories [21, 223, 304, 338], which argue that people gather information about various aspects of each choice option, assign a value to each of these aspects, trade off the different aspects, and then choose the option that maximizes their utility [34, 97, 320]. What are the aspects that people trade off in privacy decisions? Two aspects are mentioned repeatedly in existing work: perceived risk and perceived relevance.

**Perceived risk**—Privacy risk is the “potential loss of control over personal information, such as when information about you is used without your knowledge or permission” [95]. This loss of control can lead to unintended uses and distribution of the information [265, 315, 369]. The *perception of risk* is the fear that these unintended consequences will happen [148, 223]. The following research quantifies the effects of perceived risk:

- Several studies found a direct effect of perceived risk on disclosure intentions [219, 220, 262], indicating that risk perceptions may lead us to restrict access to our personal information [221, 281].
- Consumer surveys have found that between 58.2% [242] and 72% [137] of all respondents cite risk as a reason not to disclose their personal information.
- Comparing effect sizes between studies, Dinev & Hart [80] note that privacy risk may even be more likely to dissuade people from making an e-commerce transaction than the economic risk of the transaction (see also [35]).
- Extending this argument, research shows that risk may indeed influence users’ intention to transact in a web shop [172, 279], or their intention to adopt an online service [95].
- White argues that “Marketers’ efforts may be wisely directed at attempts to mitigate any perceived ‘downside risks’ associated with disclosure.” [383].

Moving specifically towards research on privacy in personalized systems, several researchers show that privacy risks may inhibit the use of such services:

- In a study on ubiquitous commerce (u-commerce), Sheng et al. [317] showed that personalization induced privacy concerns, and that users consequently would feel less inclined to use personalized (rather than non-personalized) u-commerce services, unless the benefits were overwhelming (i.e., providing help in an emergency).
- Awad and Krishnan [21] showed that users’ privacy concerns inhibited their use of personalized services and advertising.
• Sutanto et al. [342] demonstrated that privacy concerns can prevent people from using a potentially beneficial personalized application.

**Perceived relevance**—Whereas perceived risk describes the negative side of the privacy calculus, the positive side appears to be governed by the *perceived relevance* of disclosure. The following research quantifies the effects of perceived relevance:

• Stone was the first to consider the effect of the perceived relevance of information requests on privacy-related behaviors [337], and this effect has since been demonstrated empirically [219].
• Phelps et al. note that people’s purchase intentions go down when a service requests information that does not serve the purpose of the request. They therefore argue that “marketers need to resist asking for such information in situations in which the relevance is not readily apparent” [289].

In the realm of personalized services, research shows that concerns mainly exist when these services fail to provide useful benefits for which the disclosed information is relevant:

• Scientific research into consumer perceptions shows that people are willing to give up privacy for personalization [128, 265], as long as this gives them benefits [289].
• Deeper investigations into this phenomenon show that users particularly value the benefits of content relevance, time savings, enjoyment and novelty to an extent that may have them ignore their initial privacy concerns [135, 144].
• Consequently, certain researchers claim that “privacy isn’t the issue” [123] as long as the benefits are clear [174].

![Figure 1: Summary of findings from literature review of privacy decision-making](image)

Integrating these streams of research, existing work has predominantly shown that risk and relevance are both important in determining users’ willingness to adopt and provide personal
information to personalized services, and researchers therefore claim that they should both meet a certain threshold [357], or that they at least should be in balance [54, 394, 396] (see Figure 1). This finding has been depicted in Figure 2.

![Figure 2: A diagrammatic representation of users' privacy decision process.](image)

Users are not always rational; in-depth investigations are required

One critique of this existing work on the privacy-personalization paradox is that it often fails to truly investigate the tradeoff between risk and relevance as a concrete behavioral decision, because their outcome measure is a more generic form of an intention (i.e., it is measured with generic questionnaire items such as “How likely would you provide your personal information (including your location) to use the M-Coupon service?”). Such stated intentions arguably do not directly relate to observable privacy behaviors (cf. Spiekermann et al. [336] and Norberg et al. [262], who show that privacy preferences and actual behavior tend to be weakly related at best).

Indeed, the privacy calculus itself has been criticized for making unrealistic assumptions about the rationality of decision-makers [168, 169]. Rather than being rational, people’s privacy decisions are influenced by various heuristics, such as:

- Information on others’ privacy decisions (i.e. “social proof” [7])
- The order of sensitivity in which decisions are being made (“foot in the door” and “door in the face” [7])
- The overall professionalism of the privacy-setting user interface (“affect heuristic” [155])
- The available options to choose from (“context non-invariance” [185])
- The default setting and phrasing of privacy-related requests (“default” and “framing” effects [181, 204]).

Future work on disclosure behavior—including investigations of TLA users’ privacy behaviors—should conceptualize perceived risk as contextualized privacy concerns (i.e., concerns about the possible consequences of disclosing a specific piece of information to a specific recipient [70, 232, 289, 326]) and perceived relevance as contextualized benefit: the perceived benefit of disclosing a specific piece of information to a specific recipient [183, 219]. Initial work at the level
of individual privacy decisions (a yes/no decision for multiple disclosures) has been successful in separating the rational tradeoff from irrational influences, quantifying their relative contribution [7, 182, 183, 194]. The distinction between general (system-related) concerns/benefits and contextualized (information-related) risk/relevance is also depicted in Figure.

**Trust increases users’ acceptance of data collection and tracking**

Aside from highlighting the relevance of the data collection/tracking practices, there are several ways to convince users to disclose more information. Some of these methods (and their shortcomings) will be described in Section 6. Here we address the topic of trust. The following research quantifies the effect of trust on information disclosure:

- Several researchers suggest that concern/risk is a mediator between trust and disclosure intentions [232, 369, 395, 406]. This suggests that trust may reduce perceived risk, which in turn increases disclosure.
- Dinev et al. argues the opposite effect, i.e. that the effect of concern/risk is (partially) mediated by trust [79, 80]. Similarly, Knijnenburg and Kobsa showed that disclosure behavior in a demographics- and context-based recommender system was determined by trust in the company and concern/risk, with trust (partially) mediating the effect of concern/risk [182]. This suggests that trust itself can be built by reducing the perceived risk of information disclosure.
- Kobsa et al. show that trust can be a rational influence (rooted in risk and system-specific concerns) as well as a heuristic influence (rooted in the affect heuristic) [194].

Figure 2 shows the interplay between trust and concern/risk.

**Recommendations: survey users, build trust, highlight relevance**

In sum, while privacy concerns are cause for hesitation in the unfettered collection of personal information, the TLA processors rely on the collection of such information to provide accurate personalization. This leads to a *privacy-personalization paradox*, i.e., a conflict between the user’s perceived benefit of using TLA-based learning systems and their perceived concern regarding the disclosure of requisite information. The Federal Trade Committee suggests that addressing this paradox is essential for the success of personalized services [104]. Based on the analysis in this sub-section, we therefore make the following recommendations to ADL and other TLA performers:

- **Survey users**—As users’ privacy behaviors are rooted system- and context-dependent perceptions of risk and relevance, it is important to continuously measure these perceptions as TLA-based systems and their data collection practices evolve. At design-time, TLA implementers should perform scenario-based multi-factorial experiments to
quantify the effects of various data collection practices on perceived risk, perceived relevance, and disclosure behaviors. At deployment-time, they should conduct in-depth interview studies to uncover users’ privacy-related attitudes and their potentially unanticipated antecedents and consequences. Moreover, implementers should perform controlled user experiments to detect potentially deleterious effects of heuristic decision practices on users’ overall privacy concerns.

- **Build trust**—Our analysis shows that trust in the provider of a TLA-based system is an important factor in determining users’ system-specific privacy concerns and perceived disclosure risk. Trust can be built heuristically through favorable name-brand associations, and it is thus important that all providers within the interconnected network of learning applications that constitute a TLA implementation are highly trusted by its users. So, while the TLA specifications may suggest an “open” learning platform, each implementation should ensure that the learning applications originate from trustworthy sources. Trust can also be built rationally by making sure that users have minimal privacy concerns at any point of time while using the system. TLA-based systems should therefore employ sensible data collection practices and a privacy by design philosophy from the onset. The suggestions in this document are instrumental in this endeavor.

- **Highlight relevance**—The privacy-personalization paradox and the privacy calculus suggest that far-reaching data collection practices are admissible, so long as the user understands the relevance of the data collection. At every step of the way, a TLA implementation should therefore highlight the potential improvements in content relevance, time savings, enjoyment and novelty that the collection of data can provide. Section 6 discusses different means of communicating relevance to the user. Moreover, the TLA activity providers should refrain from asking for information in situations in which the relevance is not readily apparent.

1.2 Elaboration likelihood

The previous subsection demonstrated that privacy decisions are influenced by both rational and heuristic antecedents, suggesting that users sometimes elaborate on their privacy-related behaviors, while at other times take decisional shortcuts. This subsection analyzes the factors that determine the relative importance of these two types of influences. We conclude that TLA-based systems should cater to both rational and heuristic decision-making practices, and that they can try to empower users to take more active control over their privacy (see Table 4).

<table>
<thead>
<tr>
<th>Table 4: Recommendations regarding elaboration likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cater to Both Routes</strong></td>
</tr>
<tr>
<td>– Provide detailed privacy control mechanisms for central route decision-making</td>
</tr>
<tr>
<td>– Provide sensible default settings to aid peripheral route decision-making</td>
</tr>
<tr>
<td>– Provide both heuristic and rational sources of trust</td>
</tr>
<tr>
<td><strong>Empower Users</strong></td>
</tr>
<tr>
<td>– Provide contextualized controls and comic-based information</td>
</tr>
</tbody>
</table>
Users’ decision practices range from heuristic to effortful

Outside the context of privacy, the decision-making literature has long realized that users’ decision practices range from heuristic to effortful, and have attempted to create “dual process theory” models that reconcile these different types of decision processes. One such model is the Elaboration Likelihood Model (ELM) [285, 287], which argues that people—to a varying extent—use two routes of processing: a central route (high elaboration) and a peripheral route (low elaboration):

- Central route processing is most in line with the privacy calculus, as it involves a more effortful elaboration process [403], in which users form their attitudes about a product based on a careful assessment of the most relevant available information [44, 226, 286], such as objective information about risks and benefits of disclosure [15, 227, 398, 407] and the availability of advanced privacy protection mechanisms [194].
- Peripheral route processing involves a more heuristic evaluation, which relies on superficial but easily accessible cues [285, 286, 324], such as website reputation [194, 313], ostensible privacy guarantees [398, 407], and design quality [24], which is in line with the heuristic accounts of privacy decision making discussed earlier [14, 155, 222].

Users’ motivation and ability influence their elaboration likelihood

ELM specifies two variables that determine the extent to which someone uses the central or peripheral route: motivation and ability. Motivation can be a personal characteristic (i.e., certain people are just generally more motivated to make privacy decisions), or it can depend on the situation. (i.e., certain people are more motivated to make privacy decisions when the dealing with a particular type of application or a particular type of data). Similarly, the ability to process presented information can be a personal trait (i.e., certain people have more privacy knowledge) or depend on situational factors (i.e. people are likely to make more elaborate privacy decisions when they have sufficient time and no distractions) [44, 286]. The following research provides evidence for the effect of motivation and ability on elaboration likelihood in privacy decision-making:

- Privacy researchers have used general privacy concerns as a measure of one’s motivation to engage in cognitive elaboration when making privacy-related decisions [24, 194, 407]. Privacy issues are of central importance to people with high levels of concern, and those individuals will thus be more motivated to make systematic use of issue-relevant cues and information.
- People with low levels of concern, on the other hand, will be more likely to use ostensive yet superficial cues in their evaluation process [24, 194, 407]. Indeed, privacy scholars have argued that some people use shortcuts and heuristics because they are not motivated to spend the effort needed to make an elaborate decision [61].
• In a similar vein, privacy researchers have used privacy self-efficacy (a person’s belief in her cognitive resources required to cope with privacy-related problems [210]) as a measure of one’s ability to engage in cognitive elaboration of privacy-related cues and information [24, 194, 407]. People who are equipped with more knowledge and resources are more able to engage in extensive elaboration.

• In contrast, People with low levels of self-efficacy will elaborate less and are more likely to rely on decisional shortcuts [194, 324]—cues that help them decide without needing to engage in cognitively elaborate processes. Indeed, privacy scholars have argued that some people use shortcuts and heuristics because they are incapable of making an elaborate decision [225, 231].

The effect of motivation and ability on elaboration likelihood is displayed in Figure 3.

![Figure 3: The effects of ability and motivation on central and peripheral route processing in privacy decision-making.](image)

Motivation and ability can be instilled

We must acknowledge the harsh reality that users typically lack the motivation [61] and ability [225, 231] to make elaborate privacy decisions. So, while we should be careful not to overburden users with privacy control, it often serves to try and motivate and/or enable users to take a more central processing route in their privacy decision process.

One way to do this is to provide highly contextualized privacy controls, which may increase users’ self-efficacy [183] (see Section 6.2). Another way to encourage central route processing of privacy-related information is the use of privacy comics [178] (see the Section 6.1). Figure 3 further displays the (potential) effects of contextualized control and comic-based information.
In sum, TLA users may not only differ in the extent of information disclosure (as mentioned in the introduction of this section), but also in the way in which they make privacy decisions. The TLA will have to deal with users who are highly capable and motivated to make privacy-related decisions, and users for whom this is decidedly not the case. Based on the analysis in this subsection, we therefore make the following recommendations to ADL and other TLA performers:

- **Cater to both routes**—It is important to realize that not all users will be able to make elaborate privacy decisions at all times. TLA-based systems should therefore cater to both central and peripheral route privacy decision-making. For example, a TLA providers can provide detailed privacy control mechanisms for central route decision-making, but also provide sensible default settings to aid peripheral route decision-making. Similarly, TLA providers should provide both heuristic and rational sources of trust.

- **Empower users**—While this is not always possible, it is better if users make rational rather than heuristic decisions. Hence, TLA-based systems should provide contextualized controls and comic-based information in an effort to increase users’ motivation and ability to make more rational privacy-related decisions.

### 1.3 Communication style

Previous subsections covered users’ privacy behaviors towards personalized systems. However, privacy in TLA-based systems extends beyond personalization; it is also relevant to the interpersonal (“social networking”) aspects of these systems. Social networks typically provide a plethora of mechanisms to manage one’s privacy beyond disclosure [89, 390], and research finds that users tend to employ a wide variety of strategies to limit their disclosure [272, 390]. This subsection describes these strategies, and how they can be supported in a TLA-based system (see Table 5).

#### Table 5: Recommendations regarding communication style

<table>
<thead>
<tr>
<th>Tailor to Different Privacy Management Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Give Selective sharers the ability to selectively share information with specific apps and groups of people</td>
</tr>
<tr>
<td>- Give Self-Censors non-personalized mechanisms for selecting material, and restricted forms of sharing</td>
</tr>
<tr>
<td>- Allow Time Savers to opt out of active notifications and social features</td>
</tr>
<tr>
<td>- Give Privacy Maximizers all of the functionality described above</td>
</tr>
<tr>
<td>- Give privacy balancers mechanisms for curation, blocking, and avoiding direct interaction</td>
</tr>
<tr>
<td>- Make sure that Privacy Minimalists can maximally benefit from the adaptive and social functionalities of TLA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tailor to Different Communication Styles</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Employ automatic social-network style sharing for FYI communicators</td>
</tr>
<tr>
<td>- Employ direct, chat-style interaction for non-FYI communicators</td>
</tr>
<tr>
<td>- Pay special attention to effects of integrating different communication styles within a single application</td>
</tr>
</tbody>
</table>
Wisniewski et al. [389, 391] identified ten distinct privacy behaviors on Facebook: withholding basic or contact information, selective sharing through customized friend lists, blocking people, blocking apps or event invitations, restricting chat availability, limiting access to or visibility of one’s Timeline/Wall, untagging or asking a friend to take down an unwanted photo or post, and altering one’s News Feed. Moreover, they demonstrated that users use these strategies selectively. Specifically, they classified participants into six categories (see Figure 4) with distinct privacy management strategies:

- **Privacy Maximizers** use almost all of the available privacy features on the social network.
- **Self-Censors** use very few of the available privacy features, but primarily protect their privacy via the traditional method of withholding information.
- **Selective Sharers** share much more information, but they protect their privacy by sharing this content selectively, using custom friend lists.
- **Privacy Balancers** exhibit moderate levels of privacy management behaviors. Follow-up work shows that this class of SNS users contains both “informed balancers” (who carefully select the privacy mechanisms that suit their personal preferences) and “uninformed balancers” (who simply make do with the few mechanisms they are aware of).
- **Time Savers/Consumers** use Facebook primarily for passively consuming other people’s posts, and take precautions to limit or avoid direct interaction with other users (e.g. through chat).
- **Privacy Minimalists** use only a few common privacy features, but are generally very open in their disclosure.

![Figure 4: The six privacy management strategies uncovered by Wisniewski et al. [389, 391]](http://www.usabart.nl/chart)
Page et al. [270] suggests that users choose their social network based on their preferred communication style. They argue that services that broadcast implicit social signals (e.g. location-sharing social networks) are predominantly used by users who are predisposed to “FYI (For Your Information) communication”. FYI communicators prefer to keep in touch with others through posting and reading status updates, i.e., without actually having to interact with them. They tend to benefit from the implicit social interaction mechanisms provided by broadcast-based social network systems. People who are not FYI communicators, on the other hand, would rather call others, or otherwise interact with them in a more direct manner, rather than passively reading about them on social media. They thus tend to benefit more from systems that promote more direct interaction.

**Recommendation: tailor to different privacy management strategies and communication styles**

TLA users are likely to expect the system to have a wide variety of ways to communicate with other users and manage their social privacy, and that different users will use these mechanisms in different ways. Based on the analysis in this subsection, we therefore make the following recommendations to ADL and other TLA performers:

- **Tailor to different privacy management strategies**—In a recent paper [385], we explored how the different privacy management profiles uncovered by Wisniewski et al. can be applied to TLA-based systems. We refer the interested reader to the paper, and provide a summary of our analysis here:
  - Give Selective sharers the ability to curate and selectively share their personal information and training outcomes with specific applications and groups of people.
  - Give Self-Censors non-personalized mechanisms for the selection of learning material, and highly restricted forms of sharing learning outcomes.
  - Allow Time Savers to opt out of active notifications and social features.
  - Give Privacy Maximizers all of the functionality described above.
  - Give privacy balancers mechanisms for curation, blocking, and avoiding direct interaction.
  - Make sure that despite these mechanisms, Privacy Minimalists can maximally benefit from the adaptive and social functionalities of TLA.

- **Tailor to different communication styles**—As users with different communication styles prefer different mechanisms for interacting with each other, TLA-based systems should support these different mechanisms. Specifically, the TLA should employ automatic social-network style sharing for FYI communicators. These users will maximally benefit from the “social awareness” that results from seeing the implicit activity of other TLA
users. At the same time, TLA-based systems should employ direct, chat-style interaction for non-FYI communicators. This is in line with research that shows that learners are interested in seeing who is online and messaging them when they want to [399]. Since the communication styles of FYI and non-FYI communicators is at odds, user research should pay special attention to effects of integrating different communication styles within a single application.
2 Input data characteristics

Problem: What data should TLA collect? The TLA specifications envision a highly adaptive learner model that proactively mines and tracks a variety of information sources to provide personalized learning experiences. The goal of this learner model is to train employees on the job, adapting presented training modules to personal capabilities, mission requirements, and available time and other resources [98, 296]. Like many other adaptive systems, TLA-based systems thus rely on the collection of potentially privacy-sensitive information to provide its personalized learning services [105, 193, 289, 317, 342, 357, 366]. What kind of data should TLA-based systems collect, and what should they refrain from collecting?

Current state of the art: Widespread data collection envisioned. Currently, the TLA specification supplies APIs for the following kinds of user data [310, 329]:

- Learner runtime activity (Learner Experience Facts; xAPI): detailed tracking of specific learning activities
- Competency/mastery/evidence (Learner Profile; pAPI): data users’ competencies, completed objectives, evidence, expiration dates, etc.
- Learning activity descriptions (Activity Index; iAPI): most importantly, “paradata” that includes user ratings, comments, and usage statistics about the learning activity
- The learner’s context (Context; cAPI): aspects of the learner’s physical situation, computation equipment, schedule, etc.

Solution: Study the privacy implications of collecting various types of data. This section considers the privacy implications of the collection of these and other types of data by TLA-based systems. Notably, we add a discussion of social connections, physiological / psychological / medical data, skills and competences acquired outside the system, and users’ learning ambitions. It also covers the privacy implications of the potential inferences that the TLA and/or its underlying learning systems can make based on this data. Formal questions about data ownership and the transmission of data to other parties are covered Sections 4 and 5, but are referred to in this section whenever relevant.

This section describes the privacy implications of collecting data about learner activity within and outside of the learning system, with specific attention to:

- Levels of identifiability
- Collection of various data types
- Inferences made based on data collection

Key findings and recommendations are presented in Table 6.
Table 6: Key findings regarding the input data characteristics

<table>
<thead>
<tr>
<th>Levels of identifiability (2.1)</th>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Full anonymity is impossible; pseudonymous users can be re-identified</td>
<td>Use de-identification but don’t rely on it for privacy purposes</td>
</tr>
<tr>
<td></td>
<td>De-identifying server data is still a good security practice</td>
<td>Tailor users’ identifiability based on the formality of the environment</td>
</tr>
<tr>
<td></td>
<td>Pseudonymity has consequences for social interaction</td>
<td></td>
</tr>
<tr>
<td>Collection of various data types (2.2)</td>
<td>Learner runtime activity is essential for operation, but can be sensitive</td>
<td>Allow users to correct/appeal competency data</td>
</tr>
<tr>
<td></td>
<td>Continuously tracking the learner’s context can create a digital panopticon</td>
<td>Allow users to add outside skills</td>
</tr>
<tr>
<td></td>
<td>Social connection data can be used re-identify users</td>
<td>Allow users to submit their learning ambitions</td>
</tr>
<tr>
<td></td>
<td>Detailed physiological data is sensitive, and tracking it may create an unwanted power dynamic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HIPAA prohibits the collection and sharing of medical data</td>
<td></td>
</tr>
</tbody>
</table>

Inferences made based on collected data (2.3)

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users don’t like incorrect predictions</td>
<td></td>
</tr>
<tr>
<td>Even correct predictions may at times be unwanted</td>
<td>Allow users to correct and move beyond the personalized recommendations</td>
</tr>
<tr>
<td>Users are more than the sum of their data</td>
<td></td>
</tr>
</tbody>
</table>

### 2.1 Levels of identifiability

Of all the types of data that can be collected by TLA-based systems, Personally Identifiable Information (PII) deserves special attention, because the use and sharing of PII presents the risk of revealing the identity of users to other parties. PII can be defined as any information that could be used on its own or with a combination of other details to identify, contact or locate a person or to identify a person in context. The potentially classified nature of military identities makes identifiability a particularly important problem in military applications [312].

This subsection explores the limits of de-identification, and discusses the situations in which pseudonymity should be used or avoided (see Table 7).

Table 7: Recommendations regarding levels of identifiability

<table>
<thead>
<tr>
<th>Use De-Identification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use—but do not rely on—de-identification for privacy purposes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tailor Users’ Identifiability</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Creative and (self-)evaluative environments should use pseudonymity</td>
<td></td>
</tr>
<tr>
<td>Formal and diplomatic settings should enforce a real name policy</td>
<td></td>
</tr>
</tbody>
</table>
Full anonymity is impossible; pseudonymous users can be re-identified

Beyond security concerns, requesting PII also induces privacy concerns. In a seminal paper, Ackerman et al. demonstrated that most users are uncomfortable disclosing PII, such as their social security number (99%), credit card number (97%), phone number (89%), address (56%) and full name (46%)—in contrast to information that does not personally identify them, such as their favorite snack (20%) or favorite TV show (18%) [3].

A possible mitigation of these privacy concerns is to allow users to remain fully anonymous. Anonymous interaction means that there are no persistent identifiers associated with the user. Fully anonymous interaction with TLA-based systems is difficult though, since the personalization functionality inherent in the TLA specifications crucially depends on the systems’ ability to recognize the user across interactions [309]. More realistically, users can be allowed to interact with the system under a pseudonym [19, 196]. However, scholars have debated the value of de-identifying personal data stating that anonymized data may still be at risk of being re-identified [264], due to the high dimensionality and sparsity of the data typically collected by personalization learning systems [254]. In this sense, the combination of various data that are not directly personally identifiable (e.g. a combination of the user’s favorite snacks, TV shows, and other preferences) can effectively be used to identify them in a dataset. An overview of these mitigation techniques is presented in Figure 5.

This re-identification threat can be reduced by not giving others access to any of the user data. Note, though, that even without such access, it may be possible for a third party to make inferences based on the output of the system. Calandrino et al. [45] employ such a “reverse re-identification scheme” using a fake user accounts that are similar to the account of a target user. An adversary using this technique can use the recommendations provided to the fake accounts to isolate the target user’s data. A means to overcome this problem is differential privacy, a privacy model that inserts carefully calibrated noise into the user profile computation. The noise masks the influence that any difference in a particular record could have on the outcome of the computation [230, 241, 300, 408].

Interestingly, while pseudonyms and anonymity may reduce privacy concerns, many systems increasingly require users to use their real name [409] (presumably to combat the increasing number of fake accounts), and even some governments require their citizens to verify their real name before signing up on certain popular websites (presumably to counter rumors and defamation of politicians during the election cycle) [58]. A learning system that may be used to make deployment and promotion decisions may similarly require users to authenticate with their PII to prevent and combat fraudulent use (e.g. cheating). In this case, it is good practice to hash the requisite PII.
Although pseudonyms do not guarantee that users can never be re-identified, researchers have argued that de-identification of server data can be a valuable but not foolproof method for minimizing privacy and security risks. For instance, Masiello and Whitten argued that while anonymized information will always carry some risk of re-identification, most of the privacy risks occur only when there is certainty in re-identification [234]. Removing or hashing PII and introducing differential privacy introduces uncertainty in re-identification, thereby removing the most prominent privacy risks.

These mechanisms could for instance be helpful to in the instance of a data breach: Personal information such as upcoming lessons could possibly reveal where a soldier would be deployed next, which would be a privacy risk. But if the soldier’s PII is removed or hashed, and if the stored lesson data contains a certain amount of noise, then the identity of the soldier and his/her upcoming deployments cannot be determined with certainty. Targeted attacks to uncover the soldier’s PII may still succeed, but the de-identification practice prevents the data breach from...
automatically compromising the PII of all the data subjects involved in the breach. Routinely de-identifying data could also prevent rouge employees from having direct and effortless access to data that exposes the identity of users.

**Pseudonymity has consequences for social interaction**

Anonymity and pseudonymity not only influence users’ privacy; research also suggests that runtime identifiability (i.e., whether users get to know the identity of other users they interact with while using the “social” features of a system) has an influence on user behavior [316]. Specifically, in creative environments (e.g. creative thinking exercises, brainstorming activities), the absence of a name allows users to produce content more freely, which increases creativity [57, 341], reduces conformity and inhibition [60], and increases the opportunity for intimacy and the sharing of secrets [371]. The latter makes anonymity and pseudonymity useful for self- and peer evaluation exercises.

Unfortunately, pseudonymity also induces a certain dissociation between the members of an online community [341], which is obviously bad for team building exercises and other team activities. Real name requirements can avoid such problems, and have also been shown to reduce profanity and anti-normative expressions in online social networks, especially among more-frequently participating users [58]. Formal and diplomatic settings may thus benefit from a real name policy.

**Recommendation: use de-identification; tailor users’ identifiability**

Due to the intricate relationship between privacy, security, and the social consequences of pseudonymity and anonymity, it is difficult to make a simple recommendation regarding the identifiability of TLA users. Based on the analysis in this subsection, we can make the following recommendations to ADL and other TLA performers:

- **Use de-identification**—Recent re-identification threats show that simply removing or encrypting all PII in a system does not guarantee that users cannot be identified. However, de-identifying server data makes identification uncertain, which removes the most prominent privacy risks. The data storage protocols of the TLA should thus use—but do not rely on—de-identification for privacy purposes, either by not collecting any PII at all, or by removing, encrypting or securely key-coding the PII that the system is required to collected (e.g. for authentication purposes).

- **Tailor users’ identifiability**—Runtime identifiability has an influence on user behavior, with anonymity, pseudonymity and real name policies each having both desirable and undesirable social consequences. The social components of the TLA should thus use anonymity, pseudonymity, and real name policies selectively, where socially useful and appropriate. Specifically, creative and (self-)evaluative environments should use
pseudonymity, because it increases creativity and earnest. Conversely, formal and diplomatic settings should enforce a real name policy, because it reduces profanity and anti-normative expressions.

## 2.2 Collection of various data types

TLA-based systems collect a wide array of data that is used to offer learners adaptive guidance and to help teachers and institutions manage their learning ecosystem. Long-term persistent data tracking allows TLA-based systems personalize learning, build competency models, coach the learner, and discover helpful insights about its user base. Detailed in-situ tracking enables the development of increasingly smart learning activities and personal assistants that guide, coach, assess, and give feedback to learners. The collected data might even help to identify cognitive states and traits that contribute to a large number of competencies and thereby offer new generalizations of existing methods to teach and assess [310].

This subsection analyzes the privacy implications of the various data types that TLA-based systems are currently envisioned to collect and/or may collect in future iterations of the specifications (see Table 8).

**Table 8: Recommendations regarding the collection of various data types**

<table>
<thead>
<tr>
<th>Carefully Protect Learner Runtime Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Protect learner runtime activity using a combination of strict access control, encryption, de-identification and obfuscation</td>
</tr>
<tr>
<td>– Provide easy-to-use notice and control mechanisms for users to control the boundary between leisure and learning</td>
</tr>
<tr>
<td>– Test the mechanisms presented in Figure 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Treat Social Connection Data as PII</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Protect social connection data as if it were personally identifiable information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Be Careful Not to Create a Panopticon</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Reduce unfettered context tracking to prevent the creation of a digital panopticon</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Keep Some Data Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Process it and use it locally</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Users to Add Outside Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Allow users to selectively add skills and competences acquired outside the system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Users to Submit Their Learning Ambitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Provide a comprehensive manual self-reporting system</td>
</tr>
<tr>
<td>– Provide a way to test or otherwise provide evidence for skills and competences</td>
</tr>
</tbody>
</table>
Learner runtime activity is essential for operation, but can be sensitive

Tracking learner runtime activity is essential for TLA-based systems to enable personalized learning with smart learning activities. Adaptive learning modules can use runtime learning activity to track users’ abilities as they learn, and adapt the topic and difficulty level of the training to the user’s current knowledge level and pace of learning. Moreover, the analysis of highly granular learning behavior arguably allows training department managers to glean superior detailed insights about users’ overall learning progress, the effectiveness of specific training modules, and the capabilities available in their division [310]. For these reasons, users should arguably not be allowed to opt out of tracking their runtime activity, as doing so would undermine the very purpose of the TLA specifications.

Runtime activity may include very sensitive data, though. For example, detailed data from cyber range practices may reveal battlefield tactics, and training data from top diplomats may reveal weaknesses that can be exploited in negotiations. To alleviate users’ (and supervisors’) privacy concerns, these data thus need to be protected by a combination of strict access control, encryption, de-identification and obfuscation.

A complication in the tracking of runtime learner activity is the fact that tracking may occur outside the traditional learning channels; TLA-based systems can give users credit for learning other activities, such as playing a tactical game, or reading a relevant blog post. Such non-traditional learning activities blur the boundaries between leisure and learning, and require runtime learner activity tracking to be in an “always on” mode. Consequently, users may find their real-world activities tracked, which arguably more privacy-invasive (and difficult to control) than the tracking of in-system behaviors [261], especially when it happens in a pervasive and unobtrusive manner. The mining and tracking activities may also be regulated by government privacy regulations [83].

Given this fluid boundary between learning activities and real-world activities, the TLA should give the user easy-to-use notice and control mechanisms to control this boundary. Figure 6 displays five of such mechanisms, at different levels of automation:

- **Control center widget**—This mechanism uses an opt-in paradigm, as it requires users to activate the learning activity before starting it. The widget could potentially provide a time-out functionality that automatically disables the tracking after a certain time window has passed, and the widget could also automatically turn on during business hours, and off outside business hours (these options are similar to Apple’s Night Shift functionality). As an opt-in mechanism, the widget is the most private mechanism, but also the most error prone: users may forget to turn on the learning activity tracking, or may not be aware that something counts as “learning”. Compared to other mechanisms, this is the only one that does not require any background tracking.

- **Opt-in toast**—This mechanism also uses an opt-in mechanism. But it monitors users’ activity in the background to detect potential learning activities. When a learning activity
is detected, the notification appears, allowing the user to start the learner activity tracking with a single tap (alternatively, the user can ignore the pop-down toast to avoid tracking). The observed background activity used by this method (as well as the three remaining methods) does not have to be permanently stored, and it should be made clear to the user that this data is used for observation only. If client-side methods (see Section 4) are used to monitor background activity, then this data does not need to be transmitted to a server at all.

- **Opt-out toast**—This mechanism is similar to the opt-in toast, but uses an opt-out mechanism: learner activity tracking is automatically started unless the user cancels the tracking with a single tap. This mechanism is slightly more privacy sensitive, as users may overlook the notification.

- **Pop-up message**—This mechanism uses a forced-choice paradigm, as it forces users to confirm whether an activity is considered a learning activity. The automated pop-up overcomes the problem of forgetting to turn on the tracking, but the pop-up itself can be perceived as intrusive.

- **Recording banner**—This mechanism shows the user a pervasive banner to indicate that the system is recording the user’s learning activity. Tapping the banner brings the user to a screen where the recording can be ended and/or adjusted. This mechanism can be combined with any of the other mechanisms.
Figure 6: Five candidate mechanisms to control the tracking of runtime learner activity
Users should be allowed to correct/appeal competency data

Competency data is essential for research, deployment, promotion decisions. The ethical and privacy implications of using data for this purpose is discussed in Section 4. Competency data can be regarded as an aggregate form of learner runtime activity data, i.e., it only captures the outcome of a learning activity (and in some cases the evidence for this outcome). Most people feel comfortable to share such information, especially in situations where it is directly relevant [183].

Beyond that, it may also contain subjective evaluations of the user’s competence, e.g. assessments by peers, superiors, or training officers. This includes the identification of personality traits and other psychological factors [310]. The inclusion of such a subjective component requires a mechanism for users to appeal decisions or evaluations that they deem unfair or incorrect. In fact, even for objective competency data the correctness cannot always be guaranteed, so an appeals process may also be instrumental in correcting glitches in the recording of objective competencies.

Learning activity descriptions are not very sensitive

Learning activity descriptions are arguably the least sensitive type of data that TLA-based systems can collect. The main user-generated part of this data—the “paradata” that contains user feedback regarding the Learning Activities—is a type of “preference data”. Preference data can be collected in various different ways, including question-answering [257], attribute weighing [187, 189, 190], and item-based feedback—the latter can be subdivided into implicit feedback [187, 191, 299], rating [108, 173, 333], and example critiquing [56, 239, 294]. Users usually do not mind providing preference-related feedback to a system [366], but direct preference measurement is not always ideal. For example, users may not always be motivated to give explicit preference feedback [192], and their feedback may not always accurately reflect their preferences [13], especially when they are novices in the recommendation domain [187, 189]. Implicit feedback, on the other hand is easier to gather, but can result in overspecialization [191].

Research [192] shows that privacy concerns can reduce users’ intention to give explicit preference feedback, but that this intention will increase with choice satisfaction and system effectiveness. In other words, a responsive adaptive system can overcome privacy concerns and encourage users to contribute preference information. Privacy concerns regarding implicit tracking of preferences (e.g. by monitoring recommendation browsing behavior) are also low: recent research found that between 80% [194] and 87% [182] of users allow this type of tracking.
The field of context-aware recommender systems has shown that context information (such as a user's interaction with other users, location, calendar events, etc.) can be used to improve the accuracy of predictions about users’ tastes and preferences, which could improve the personalized presentation of learning activities [10]. Context can also be used to adapt the presentation of the current learning activity to the user’s situation [100, 310, 399].

One benefit of context data is that it can be collected continuously and unobtrusively (compared to e.g. users’ demographics or preferences, which may have to be explicitly elicited) [215]. This is at the same time also the biggest problem of context data, because it has been shown that users are more concerned about personal information that is collected automatically compared to manually provided information [182, 184, 194]. Particularly, users fear that the system could make incorrect inferences about their situation, or use the collected data for unintended purposes. While users are relatively okay with an adaptive system tracking their location (85%), phone model (85%), and general app usage (82%), they are much less willing to have an app track their Web browsing (48%), email messages (37%) and mobile credit card purchases (20%) [182].

An important reason for users’ worries is that the system may make incorrect inferences based on the data [182], or that the system may reveal embarrassing contextual information to other users of the system [272]. Another problem with context data is that it typically concerns behavior that is not directly representative of users' tastes and preferences, which makes it difficult for the system to highlight its relevance. Since context tracking is not essential for the correct operation of the core TLA-based personalization services, users should be allowed to opt out of continuous context tracking (or, alternatively, context tracking should be disabled by default, allowing users to opt in for a better personalized experience; see Section 6.3).

The continuous tracking of the learner’s context makes it more difficult for users to lie about their activities and whereabouts [126]. While increasing honesty may seem like a desirable goal, studies in computer-mediated interactions show that users sometimes lie as a privacy preservation tactic [125]. A user may for example tell a friend that she has fallen ill, rather than telling the friend that she does not want to go out with her that evening [271]. Researchers recommend that social information systems allow users to make white lies; a functionality that has been dubbed “plausible deniability” [17, 36, 213]. Page et al. [271] demonstrate that in systems that create a “panopticon” (cf. [22, 298]) by pervasively tracking, the practice of lying indeed increases the privacy concerns of the liar. The problem of lying in information systems is a complex issue that involves balancing the opportunity for users to lie with the moral responsibility of creating honest digital experiences. TLA developers need to be acutely aware of this issue, since TLA-based systems may expose—or further exacerbate—users' lies.
Social connection data can be used re-identify users

Access to social connection data allows TLA learning applications to create powerful collaborative or competitive social learning experiences. The privacy implications of such experiences are discussed in Section 5.2. Here we consider the privacy of the social connection data itself.

In an increasingly networked world, it is important to realize that social connection data can reveal a lot of information about a user. Indeed, social connection data can be used to re-identify anonymous users [253], and “neighborhood attacks” can be used to infer unrevealed traits about a user from friends’ traits [404, 405].

Detailed physiological data is sensitive, and tracking it may create an unwanted power dynamic

Leveraging novel sensing technologies that are increasingly incorporated into consumer devices, TLA-based systems could potentially have continuous access to a wide range of physiological metrics, such as sleep patterns, weight, physical exertion, and heart rate. Detailed runtime physiological tracking can be used to make real-time adjustments to combat and fitness training routines, pushing users to—and beyond—their personal limits. Moreover, in aggregate, such data allow TLA-based systems to track the health of its users, and recommend physical training programs that match their current physical condition. Knowing users’ overall health and fitness also supports supervisors’ deployment decisions.

An increasingly interesting use of physiological sensing technology is biometric authentication [76]. TLA-based applications could use this method to provide access to authorized personnel without the need for passwords. Note that some forms of biometric authorization, such as face scans [75], fingerprints [149], and iris scans [247], can be compromised with the right tools.

It remains a question whether TLA users will feel comfortable with having the system tracking their biometrics and physiological activity. Studies show that relationships between different types of physiological data can give very detailed insights into the user’s life [122], so these tracking applications and wearable devices are rapidly becoming an important source of privacy and security leaks [26, 121]. Insights into the user’s sexual activity and bodily functions can for example be gleaned from this type of data [26]; users may not want such information to be available to their employers. Aggregation reduces these problems. We therefore suggest a hybrid solution where detailed runtime physiological data is used for adaptations at the client side only, and aggregated before transferring it to the server, where it is used for tracking users’ general health and physical condition (see also Section 4).

Surveying research on pervasive tracking in elderly care, Alemdar and Ersoy find that the use of sensors creates an interesting power dynamic: while the monitoring benefits the elderly as well
as the people taking care of them, only the elderly themselves suffer the downsides of constantly being monitored [11]. Analogously, the pervasive tracking of physiological activity may create an unwanted power dynamic between users and their supervisors. To wit, the military already places important restrictions on soldier’s activities, and strong demands their physique, for the purpose of combat preparedness [372]. While continuous tracking may support a soldier in pushing their boundaries and striving for perfection, it also creates an implicit expectation of 24/7 commitment to such goals, which can be a source of unwanted pressure which can negatively impact the employee and their family [382]. This can be countered by increasing employee choice and flexibility over work demands.

**HIPAA prohibits the collection and sharing of medical data**

As an extension beyond physiological data, TLA researchers could help identify, prevent, and or mitigate health risks. Platforms such as Apple’s HealthKit and WebMD demonstrate that basic online diagnosis of health issues is becoming more prevalent today [99, 109]. This could be a useful feature for users working in areas where contagious diseases are common, or in remote locations without access to medical care. TLA-based learning systems would also benefit from having applications that educate users about personalized preventative health practices. Such applications could also obtain input from the user to help them identify any ailments they may be suffering from [82, 249]. Finally, such functionality could reduce some of the immense pressure on the Veterans Affairs to care for veterans’ medical health.

As the HIPAA privacy law [15] prohibits the sharing of medical information with employers and other third parties, such applications should be accessed only by the user and should under no circumstances be shared with their employer. Client-side methods could be used to implement this requirement (see also Section 4).

**Allow users to add skills and competences acquired outside the system**

TLA users may have skills and competences that were not acquired under the auspices of TLA, either because these skills were acquired before they became TLA users, or because they were acquired through learning applications that are not part of TLA. Users may want to “import” these skills and competences into their TLA-based system to demonstrate their diverse skillset to their employer (e.g. for promotion purposes). Likewise, for TLA-based systems it is also useful to be aware of these skills and competences. Indeed, the design rationale for TLA envisions it to be fully backwards compatible with traditional LMS-based learning environments [310].

Note that users might not want to input all the skills they have acquired outside TLA. For example, users may fear that a skill they acquired at a previous job but that is not aligned with their current interests may inadvertently cause their supervisor to change their current job to make use of these other skills. One way to resolve this problem is to allow users to **selectively**
add previously-acquired skills. Another resolution lies in the ethical dilemma of the tradeoff between organizational needs and users’ personal interests. This dilemma is further discussed in Section 5.3.

Allow users to submit their learning ambitions

As adaptive systems become increasingly more common, there exists a fear of “over-automation” and loss of control among their users [208, 275]. In TLA-based adaptive learning systems, this could cause a loss of perceived ownership over the user’s learning process—a situation that may reduce users’ motivation and learning effectiveness. In response to this problem, recent research has suggested to give users of adaptive decision support systems a more meaningful role in the decision-making process [188]. TLA-based systems could promote a similar philosophy, by allowing users to submit their learning ambitions (e.g. whether the user would like to build a specific specialization, or transition into a management position), and take these into account in providing learning recommendations. Arguably, a system that acknowledges these ambitions can leverage users’ intrinsic motivation to learn, which is much more powerful mechanism than extrinsic motivation (e.g. recognition, promotion) [77]. This idea requires an ethical discussion of the tradeoff between these ambitions and organizational needs, which is provided in Section 5.3).

Recommendation: treat each data type in an appropriate manner

TLA-based systems may collect a wide variety of input data to provide personalized learning experiences. Each type of data should carefully be considered in an appropriate manner. Based on the analysis in this subsection, we can make the following specific recommendations to ADL and other TLA performers:

- Carefully protect learner runtime activity—Learner runtime activity can reveal a lot of sensitive details about users, and compromise security. It is therefore important to protect learner runtime activity using a combination of strict access control, encryption, de-identification and obfuscation. This learner activity may overlap with leisure activity, so the TLA should provide easy-to-use notice and control mechanisms for users to control the boundary between leisure and learning. To this goal, we recommend conducting a user experiment to test the mechanisms presented in Figure 6.

- Treat social connection data as PII—Social connection data can be used to re-identify users. The TLA should thus protect social connection data as if it were personally identifiable information.

- Be careful not to create a panopticon—Context tracking and pervasive monitoring of physiological data may improve personalization, but it also restricts user freedom. The TLA should reduce unfettered context tracking to prevent the creation of a digital panopticon.
• **Keep some data local**—Fine-grained physiological data can be very revealing about users’ most personal activities, so users may not want to share it. HIPAA prevents medical data from being shared. If learning applications want to take advantage of this data, they should process and use it locally (i.e., on the user’s device).

• **Allow users to add outside skills**—Not all skills and competences are acquired within the context of the TLA. The system may still benefit from knowing about these skills and competences. To the extent that users want to share this data, the TLA should allow users to selectively add skills and competences acquired outside the system.

• **Allow users to submit their learning ambitions**—A system that acknowledges these users’ ambitions can leverage their intrinsic motivation. The TLA should thus provide a comprehensive manual self-reporting system. It should possibly also provide a way to test or otherwise provide evidence for skills and competences the user claims to have acquired outside the TLA.

### 2.3 Inferences made based on collected data

As the previous subsection has already alluded to, the privacy implications of data collection in personalized systems extend beyond the collected data itself, to the potential (and actual) inferences the TLA Processors are able to make based on the combination of different data sources. Users are intuitively aware of this threat of aggregation, and indeed seem to get increasingly wary as disclosures accumulate within a given system [27, 182, 202].

This subsection analyzes the impact of automatic inferences on users’ privacy. Our main recommendation is to allow users to scrutinize and correct inferences made by the personalized learning system, and to give them a more active role in the process of curating learning activities (see Table 9).

**Table 9: Recommendations regarding inferences made based on collected data**

<table>
<thead>
<tr>
<th>Allow Scrutiny and Corrections</th>
<th>Build Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Give users the opportunity to scrutinize and correct potential mistakes</td>
<td>– Allow users to venture beyond the personalized recommendations</td>
</tr>
<tr>
<td>– Give TLA users a more meaningful role in the decision-making process</td>
<td></td>
</tr>
</tbody>
</table>

**Users don’t like incorrect predictions**

First and foremost, users get annoyed when personalized systems make an incorrect prediction or inference about them [326]. One famous example of this involved a man whose TiVo (a digital video recorder with a built-in recommender system) started exclusively recording TV shows with Gay themes [402]—arguably after “overfitting” a previously encountered information pattern [299]. In the TLA incorrect predictions can lead to the system recommending a training at the wrong difficulty level (which in some cases may lead to physical injuries), presenting a training in
a modality that does not match the user’s context (e.g. presenting video-based learning material while the user is driving, or an audiobook in a noisy environment), or presenting training material that does not match the user’s preferences or learning goals (leading to boredom and wasted time). Moreover, incorrectly stereotyped recommendations can lead to embarrassing situations when other people (e.g. team members or classmates) get to observe these recommendations. Users typically have an urge to correct and/or compensate for mistaken predictions [65]. In effect, researchers suggest that users should have the opportunity to scrutinize [163] and correct [103] potential mistakes.

**Even correct predictions may at times be unwanted**

Even when inferences are correct, they may not always be in the user’s best interest. Some of the recommendations that the TLA Processors will be able to make may simply be perceived as “creepy” [318, 348]. For example, Phelan et al. find that Facebook users intuitively dislike the fact that their data is being tracked, even if they have no rational objections against it [288]. This intuitive dislike may reduce users’ trust in the system.

Moreover, the use of data that to most users deem innocuous in isolation (e.g. preferences [3]) may in aggregate result in inferences about personality or lifestyle that the user is uncomfortable disclosing. For example, it has been shown to be possible to predict someone’s sexual orientation based on 5-10 Facebook likes [200]. A related fear is that such inferences might transpire in the user’s recommendations, which, if consumed in the presence of others, may “out” the user. Examples of this are the secretly pregnant teenager who received personalized Target baby advertisement brochures at her parents’ address [84], and the closeted lesbian mom whose private Netflix viewing history was re-identified using her public IMDB profile [256].

Another problem is that stereotypical inferences could result in discriminatory practices. For example, the TLA specifications envision data mining capabilities that might be able to identify cognitive states and traits that contribute to a large number of competencies, thereby offering new generalizations of existing methods to teach and assess [310]. The fear is that such data could be used in a negative sense as well. For example, Schneider et al. ask “What if that Soldier misses out on a promotion, key assignment, award, or superior evaluation because the algorithm has determined that he is at risk for suicide-related behavior? Is this outcome fair? Does it violate the Soldier’s right to privacy? Will uninformed use of this data actually increase the Soldier’s risk of self-harm?” [312]. Section 5.3 provides an ethical discussion of the use of such data, which is a first step in answering these questions.

**Users are more than the sum of their data**

It is important for realize that predictions made by TLA-based systems may never be perfect, because users are more than the sum of their data. This means that the personalization aspects
of the TLA specifications should not be taken too far, and that users should always be able to venture beyond the personally recommended content. Indeed, researchers have argued that heavily filtered content may isolate us from a diversity of viewpoints, content, and experiences, and thus make us less likely to discover and learn new things (a phenomenon known as the “Filter Bubble” [275]). The Filter Bubble can be thought of as a privacy threat because it intrudes upon our ability to experience the world from an unbiased perspective [330]. When users are encouraged to follow the recommendations of their adaptive learning system, stereotyping can even create a “positive feedback loop” [208], where users increasingly try to fit the stereotype. This leads to a very worrying concern that recommender algorithms may gradually replace human creativity and understanding; a scenario reminiscent of the seminal privacy novel 1984 [267]. As mentioned earlier, a good remedy against this concern is to give users of adaptive decision support systems a more meaningful role in the decision-making process [188].

**Recommendation:** Allow users to correct and move beyond the personalized recommendations

In sum, users may not always welcome the inferences their adaptive learning system may make based on the available input data, regardless of whether these inferences are correct or not. TLA-based personalized system should thus recognize the limitations of personalization, and allow users to more actively engage with the system and its content. Based on the analysis in this subsection, we can make the following recommendations to ADL and other TLA performers:

- **Allow scrutiny and corrections**—Providing users a personalized learning experiences will not be without problems. The TLA Processors may make incorrect predictions, or predictions that users may be uncomfortable with. TLA-based systems should therefore give users the opportunity to scrutinize and correct potential mistakes in their predictions.

- **Support self-actualization**—As people tend benefit from exploring their interests beyond the beaten path, TLA-based systems should allow users to venture beyond the personalized recommendations. One way to support this is to give TLA users a more meaningful role in the decision-making process.
3 Output characteristics

Problem: How should TLA present adaptations? As TLA envisions both adaptations about apps (meta-adaptations) as well as within apps (macro- and micro-adaptations), the TLA Providers should coordinate the presentation of adaptations to create a consistent experience throughout the learning architecture. What should these adaptations look like, and how should they be timed, so that users experience minimal intrusion from these adaptations?

Current state of the art: Very little work on adaptation presentation. The TLA architecture specifies three types of adaptations [329]:

- Meta-adaptations are individualized recommendations to switch from one Learner Activity to another that are based on the learner’s specific needs and progress.
- Macro-adaptations determine the next learning activity inside a single activity provider.
- Micro-adaptations adapt learning content within a single learning activity.

For users, such adaptations make it easier to find Learning Activities and activity providers that fit their current needs, and help them explore and expand their learning interests. For User Facing Application developers, good adaptations result in trust and continued use. To be efficient and useful for both parties, the adaptation mechanism needs to be accurate without being intrusive or inconvenient. However, very little work to date has considered the presentation of adaptations as a main focus of user-centric research [176, 179].

Solution: Study the timing and presentation of adaptations. The previous section discussed the intrusiveness of various types of input data; this section describes factors that impact the effectiveness of recommendations and adaptations within and across learning activities, including:

- Adaptation and presentation mechanisms
- Output modalities and devices

We discuss the convenience (or potential inconvenience) caused by the recommendations themselves. Specifically, we argue that adaptations should be:

- Carefully timed, potentially based on contextual input regarding the interruptability of the user.
- Carefully explained, without being overly persuasive.
- Conservative in how much information they provide, limiting the potential for leaking classified information.

Key findings and recommendations are presented in Table 10.
### Table 10: Key findings regarding the output characteristics

<table>
<thead>
<tr>
<th>Adaptation and presentation mechanisms (3.1)</th>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Adoptions can serve multiple purposes</td>
<td>Provide multi-purpose adaptations</td>
</tr>
<tr>
<td></td>
<td>Recommendations can be “pushed” by the user or “pulled” to the user</td>
<td>Carefully time pushed recommendations</td>
</tr>
<tr>
<td></td>
<td>Explanations can persuade users to follow recommendations</td>
<td>Explain recommendations without being overly persuasive</td>
</tr>
<tr>
<td>Output modalities and devices (3.2)</td>
<td>Smartphones are ideal for Just-In-Time learning, but can be distracting</td>
<td>Do not disturb the user</td>
</tr>
<tr>
<td></td>
<td>Wearables are less disruptive, but may feel more intrusive</td>
<td>Prevent leaking information in social settings</td>
</tr>
<tr>
<td></td>
<td>Notifications can leak personal information</td>
<td></td>
</tr>
</tbody>
</table>

### 3.1 Adaptation and presentation mechanisms

Making correct inferences about the user is only half the job of an adaptive system: those inferences need to be turned into actionable adaptations, and presented to the user in a way that is impactful but not intrusive or overly persuasive.

This subsection deals with the best presentation mechanisms for multi-purpose adaptations. We argue that adaptations should be presented timely, explained carefully, and that apps should avoid pressuring users into engaging into learning activities they do not want to engage in (see Table 11).

### Table 11: Recommendations regarding adaptation and presentation mechanisms

<table>
<thead>
<tr>
<th>Provide Multi-Purpose Adaptations</th>
<th>Carefully balance different adaptation purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allow users to weight adaptation purposes</td>
</tr>
<tr>
<td>Carefully Time Pushed Recommendations</td>
<td>Use (client-side) context-awareness to detect the optimal time to make a recommendation</td>
</tr>
<tr>
<td></td>
<td>Provide users with timely feedback about their learning performance</td>
</tr>
<tr>
<td>Explain Recommendations Without Being Overly Persuasive</td>
<td>Explain the implemented adaptations to the users</td>
</tr>
<tr>
<td></td>
<td>Avoid pressuring the users into accepting adaptations that they do not want to accept</td>
</tr>
<tr>
<td></td>
<td>Give users various options to choose from and help them understand the value of each option</td>
</tr>
</tbody>
</table>

**Adaptations can serve multiple purposes**

Recommender systems typically model their recommendations after users’ predicted behaviors or preferences. In a learning environment, adaptations can be based on suggested lesson sequences, user goals, team needs, or mission objectives. In other words, the adaptations serve multiple purposes, both from the users’ viewpoint as well as the providers’ viewpoint [152]. In
line with Jannach and Adomavicius’ “Purposeful Evaluation Framework” [152], Table 12 illustrates the learning tasks that TLA-based adaptations can support.

The different learning purposes are not always aligned. Promoting behavioral change means breaking with users’ current preferences, and creating group consensus may mean individual users have to compromise.

Even focusing on the users’ preferences, it is possible that the users’ current behaviors and future aspirations are not aligned [88], or that their current preferences are uninformed due to the limited viewpoint that their “filter bubble” provides [208, 275]. As such, adaptations could focus on allowing users to explore and understand their own learning preferences, rather than replacing this process algorithmically [188]. Giving users an active role in deciding what to learn reduces their dependency on the TLA. Moreover, it will likely result in a more thorough understanding of a user’s learning preferences, something that is very useful since users’ learning preferences are typically not singular, but rather multi-faceted and only loosely connected [151].

Table 12: User tasks TLA-based adaptations can support

<table>
<thead>
<tr>
<th>Item/User Task</th>
<th>Description</th>
<th>Generic Recommender</th>
<th>TLA Recommender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploration</td>
<td>Proposing things that vary from current preferences</td>
<td>Proposing a new song from a genre the user usually does not listen to</td>
<td>Proposing a course on a topic the user is not yet familiar with</td>
</tr>
<tr>
<td>Recommended Sequence</td>
<td>Recommending the best sequence of items</td>
<td>Recommending a sequence of books</td>
<td>Recommending a daily “couch to 5K” training sequence</td>
</tr>
<tr>
<td>Finding a better fit</td>
<td>Suggesting things that better aligns with users’ goals</td>
<td>Suggesting a movie based on the plot keywords of previous choices</td>
<td>Suggesting a more detailed security course for a security expert</td>
</tr>
<tr>
<td>Goal Oriented</td>
<td>Making a suggestion with the purpose of changing users’ behavior</td>
<td>Suggesting the user to increase their workout goals</td>
<td>Suggesting the user to take a more challenging course</td>
</tr>
<tr>
<td>Promoting behavioral</td>
<td>Supporting users while they complete other tasks</td>
<td>Suggesting alternative shirts to the one being displayed</td>
<td>Recording an ad-hoc Learning Activity</td>
</tr>
<tr>
<td>change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task Specific</td>
<td>Recommending novel items</td>
<td>Recommending breaking news articles</td>
<td>Recommending a new training program</td>
</tr>
<tr>
<td>Novelty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Context Specific</td>
<td>Recommending different learning styles or methods</td>
<td>Recommending a restaurant nearby</td>
<td>Recommending an audio-based training when the user is driving</td>
</tr>
</tbody>
</table>

Recommendations can be “pulled” by the user or “pushed” to the user

Traditionally, recommendations are requested by the user, e.g. via search or navigation [41]. User-requested recommendations are usually shown on a page, e.g. a “Top-N” [78] or as “related items” [224]. Importantly, such recommendations do not get pushed to the users; rather, users “pull” these learning recommendations by visiting a portal (e.g. meta-adaptations can be made to Learning Activities that are presented a learning “App Store”).
Alternatively, a recommender system can “push” adaptations to the user using mobile technologies such as text messages or smartphone notifications. Pushed adaptations have the advantage of being timely (i.e. they support Just-In-Time learning [310]). Moreover, they are more suitable for recommending sequences, and can more easily adapt themselves to the task and context (see Table 12). That said, it is harder to give users a choice when using push-based recommendations, and research shows that users’ privacy concerns for push-based adaptations are significantly higher than for pull-based adaptations [396].

Timing is an important aspect of push-based recommendations [203, 290, 306, 361]. Specifically, recommendations should be made only when users are available, e.g. when they are transitioning from one task to the next [71, 72]. Complex adaptive methods exist for determining when users are most interruptable [141].

Timing is also important for giving users feedback about their performance on a certain Learning Activity. Giving users clear and timely feedback about their performance maximizes their potential to learn from their mistakes, reduces evaluation anxiety, and increases users’ trust in the system’s subsequent recommendations.

Adaptations are only useful if the user cares to listen to them, and in many cases this means that they need to be carefully explained. The ability to effectively explain results or reasoning could be incredibly important for TLA users when they are faced with difficult choices. Explanations contribute to increased levels of perceived system competency by making interfaces easier to use, understand, and trust [293, 354, 373].

An example of how explanations could be used within TLA is illustrated using PERLS. Figure 7 shows an ‘action card’ that persuades learners to set goals. Using the explanatory criteria mentioned above, the interface allows transparency in explaining how the recommendation was chosen using a conversational tone that users can connect with. The interface also has a very prominent design. The ‘action card’ is salient as it is the only item being shown on the screen and which increases the effectiveness of the recommendation. The framing of the recommendation is also very persuasive, which may be helpful for some learners but annoying for others.

---

Note that email is an intermediate format between “push” and “pull”-based recommendations.
Knijnenburg [176] argues that explanations of adaptive functionalities can be provided by a human-like agent. They argue that the benefits of a human-like character can be twofold: Firstly, an agent can explicitly explain the occurrence of an adaptation, by stating what has changed and why it changed. But more importantly, an agent implicitly explains the adaptive behavior by representing the autonomous behavior of the system. When an adaptation is made, the agent can explain that it, instead of the system, performed the change. The agent then appears to be an autonomous body that monitors the users’ interaction, reasons about their domain knowledge and choice goals, and adjusts the system accordingly. In other words, its human-like appearance can be used as an instant metaphor for autonomy and intelligent adaptiveness. The initial results of Knijnenburg’s study show, however, that virtual agents had a negative effect on the acceptability of adaptation explanations.

An important caveat to explanations is that system developers should be careful not to “nudge” users into the direction of the recommendation too forcefully, especially when the recommendation serves purposes other than the user’s own benefit. Adaptations have much in common with nudges (see Section 6.3), in that they provide a subtle yet persuasive cue or suggestion regarding the optimal user behavior [349]. Like nudges, recommendations have been shown to have persuasive qualities [67, 179]: users are prone to agree with a recommender’s predicted ratings [65] and to follow its advice [115]. This creates a “positive feedback loop” [275]: rather than going through the trouble of developing our own unique taste, we take the default setting and simply consume whatever the system serves us [188]. This consequence of “soft paternalism” has been criticized by both decision theorists and privacy scholars for violating the user’s right to make their own decision [327, 332]. To avoid such criticism, recommendations should be framed in a way that expands rather than restricts the user’s choice options. Using this
philosophy, careful explanations may actually empower users to make better decisions on their own.

**Recommendation:** Provide carefully timed, well-explained, multi-purpose adaptations

Adaptations can serve multiple purposes, not all of which are in service of the user themselves. It is therefore important not to “shove these adaptations down the user’s throat”, but instead respectfully involve the user in the recommendation process. Based on the analysis in this subsection, we can make the following recommendations to ADL and other TLA performers:

- **Provide multi-purpose adaptations**—The TLA Providers, which calculate and distribute adaptations, should carefully balance different adaptation purposes. Different adaptation purposes may conflict with each other. Therefore, if possible, the TLA providers should allow users to weigh adaptation purposes relative to one another.
- **Carefully time pushed recommendations**—Pushing recommendations may be more appropriate for Just-In-Time learning than requiring users to pull them. User Facing Apps should use (client-side) context-awareness to detect the optimal time to make a recommendation, to not bother users when they are busy. Likewise, apps should avoid building up evaluation anxiety, and provide users with timely feedback about their learning performance.
- **Explain recommendations without being overly persuasive**—To increase trust and confidence, apps should explain the implemented adaptations to the users. However, while apps may make recommendations with the purpose of promoting behavioral change, their explanations should avoid pressuring users into accepting adaptations that they do not want to accept, and rather give users various options to choose from and help them understand the value of each option.

### 3.2 Output modalities and devices

TLA-enabled learning experiences are envisioned to be multi-device experiences [106] including smartphones, smart TVs, eBooks, smart watches, and a multitude of other devices. The meta- and macro-adaptations provided by TLA-based applications can also be pushed to (or accessed by) the user through these various devices.

This subsection discusses the pros and cons of using different devices for the display of Learning Activity recommendations (meta- and macro-adaptations). We suggest that notifications of such recommendations should be planned carefully, so as to not intrude upon users’ privacy and/or leak potentially classified learning activities (see Table 13).
### Table 13: Recommendations regarding output modalities and devices

<table>
<thead>
<tr>
<th>Do Not Disturb the User</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Plan notifications carefully</td>
</tr>
<tr>
<td>− Do not interrupt a user’s current task</td>
</tr>
<tr>
<td>− Provide easy controls for notification urgency</td>
</tr>
<tr>
<td>− Adapt notification timing to the user’s context</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prevent Leaking Personal Information in Social Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>− Provide generic notifications that do not reveal (potentially classified) details</td>
</tr>
<tr>
<td>− Change the amount of information provided in each notification depending on the number</td>
</tr>
<tr>
<td>of people that are near the user</td>
</tr>
</tbody>
</table>

**Smartphones are an ideal device for Just-In-Time learning, but can be distracting**

Seventy-two percent of U.S. adults own a smartphone (slightly above the average of 68% in advanced economies) [292]. Smartphones are ideal for providing notifications, updates, schedule changes, and other information to users almost instantly, since most people carry their smartphones with them. This makes smartphones an ideal device for learning, and researchers have indeed made a push for using smartphones in what has been called “m-learning” [139].

A TLA-specification based learning system can provide users with trainings, information and personalized Learning Activity recommendations (i.e. meta- and macro-adaptations) anywhere and anytime. This ubiquitous availability allows for Just-In-Time learning, and is ideal for users who are not bound to a specific location to do their work [310]. If any new Learning Activity recommendations or scheduled trainings become available, they can appear instantly on all users’ phones.

Another benefit of having a learning system on users’ smartphones, is that the smartphone sensors can be used to contextualize individual Learning Activities (i.e. micro-adaptations). For example, the smartphone can find out whether the user is on the move (GPS), walking or driving (accelerometer), or in a crowded environment (microphone), and adjust the training recommendations accordingly. If users maintain other information on their smartphone as well (e.g. their calendar, social networks, and email), adaptations can use this information to inform adaptations as well. Such context-aware recommendations [10] can be very powerful, but they can also result in privacy issues [182] (see Section 2.2).

Another problem is that notifications can cause unwanted interruptions of existing tasks [203, 290, 306, 361]. In the previous subsection we therefore suggested to time notifications carefully, based on contextual cues [71, 72].
**Wearables are less disruptive, but may feel more intrusive**

Wearables are a more recent advancement in mobile technology that can be used for learning applications [101]. We discuss the privacy implications of tracking health data through wearable technology in Section 2.2. Here we focus on the ability of wearables to notify users of available Learning Activities. Smart watches are ideally suitable for this purpose. Glancing at a notification on a smart watch is less disruptive than having to look at one’s phone, but such notifications are also harder to ignore. Moreover, a smart watch screen is small, so conveying detailed information and making privacy and interruptibility settings is challenging [250].

Apple has created several settings for its watch to reduce intrusiveness, including a Silent Mode, Do Not Disturb, and most recently Theatre Mode [29, 263] (see Figure 8). These settings allow users to receive notifications with a level of urgency that matches their current activity. Like with smartphones, adaptive methods to detect interruptibility would shift some of the burden of managing notification intrusiveness from the user to the device itself [71, 72].

![Apple's Silent Mode and Do Not Disturb features](image)

**Figure 8: Apple's Silent Mode and Do Not Disturb features**

**Notifications can leak personal information**

TLA-based applications should take care not to “leak” personal information through their notifications. Overly public notifications can lead to security threats and embarrassing situations when other people (e.g. family members or visitors) get to observe these notifications [40]. Having the option to control how particular devices notify users of recommendations could avoid potential leakage of personal information.

For example, notifications could be muted when displayed on a communal display device (e.g. a smart TV) or played over a set of speakers (e.g. in the car). Rather than announcing “Would you like to start reading a newly available e-book on combat in the middle east?”, which reveals a (potentially classified) learning goal of the user, the system could prompt the user by first
announcing that there is an update, allowing the user to respond to get more details or
alternatively to dismiss the notification.

Similar mechanisms can be used to address privacy for shared devices [127], and to address
privacy for mobile devices in the case of “shoulder surfing” [132].

**Recommendation:** adapt notifications to the user’s context

The TLA is envisioned to support a multitude of devices for the consumption of Learning
Activities. These devices can also be used to notify users for activity recommendations (meta-
and macro-adaptations). In this subsection, we argued that these notifications should be “smart”
or adaptive themselves as well. Specifically, based on the analysis in this subsection, we can
make the following recommendations to ADL and other TLA performers:

- **Do not disturb the user**—Smartphones and smartwatches provide a means to push
  adaptations to users instantly. TLA End User Application developers should plan
  notifications carefully, so that they do not interrupt users’ current task. Systems can
  either provide easy controls for notification urgency, or adapt notification timing to the
  user’s context.
- **Prevent leaking personal information in social settings**—TLA-based apps may be used
  on devices that are visible to, or shared by, multiple people. In such situations, systems
  should provide generic notifications that do not reveal (potentially classified) details
  unless the user asks for them. Again, systems can use contextual cues to measure the
  social setting, and change the amount of information provided in each notification
  depending on the number of people that are near the user.
4 Data location and ownership

Problem: Who owns the data, and where does it reside? The TLA specifications enable the creation of distributed learning systems that are inherently decentralized in nature. This raises questions about where exactly the collected data resides, and which components can access and process this data. Moreover, it raises questions about who owns the training data and user models that are collected and constructed by the ecosystem of connected learning applications.

Current state of the art: No clear specification of data location and ownership. The standardized web service specifications that comprise TLA are explicitly developed for assembling component products into enterprise e-learning solutions. They provide a decentralized means to connect external learning applications, augmented with a layer of data collection and adaptation. This allows developers in creating ecosystems for self-directed life-long learners who expand their competences as they progress through their career [310]. Within these ecosystems, data is stored in the “TLA Data Core”, which accumulates the data collected by various applications, and subsequently allows these applications (and the TLA Processors) to use this data for adaptation purposes (Figure 9). Questions of ownership, usage rights, and storage (beyond the central TLA Data Core) remain unanswered in the existing specifications [310].

Solution: Specifically address questions of location and ownership in the TLA architectural specification. This section addresses these questions of data location and ownership from a user-privacy perspective—in addition to discussing the effects of privacy-preserving solutions on the system's security and adaptation capabilities—through:

- Managing meta-, macro-, and micro-adaptations
- Data ownership and stewardship

We conclude by building access control for macro-adaptations and client-side methods for micro-adaptations directly into the TLA architectural specifications. Key findings and recommendations are presented in Table 14.
### 4.1 Managing meta-, macro-, and micro-adaptations

This subsection discusses the various ways in which TLA can implement its data collection and storage facilities, addresses the adaptation capabilities they rule out or enable, and analyzes their impact on users’ privacy perceptions. Essentially, the TLA has three components that are relevant to the collection, storage, and processing of personal information [329] (see Figure 9):

- **The TLA Data Core** stores all the data collected from the user, including Learner Experience Facts, the Learner Profile, and Context data.
- **The TLA Processors** provide centralized meta-adaptation capabilities on top of the data core. In this setup, individual learning applications use personalization as a service [119, 374] through the aAPI.
- **Individual learning applications**, known as **User Facing Apps** generate data about the user that feeds into the data core through the xAPI. These apps may also provide their own macro- and microadaptations, thereby creating a distributed personalization architecture. This architecture either requires each application to access the TLA Data Core through the xAPI and the cAPI.

This subsection outlines the benefits and drawbacks of this adaptation approach, and then proposes a hybrid architecture that uses the current mechanism of TLA processors for meta-adaptations (using the aAPI), specifies a privacy-controlled distributed personalization architecture for macro-adaptations (clamping down on the xAPI), and requires context-based micro-adaptations to be implemented on the client-side, thereby avoiding the need to collect granular runtime learner activity data and context data (see Table 15).

---

**Table 14: Key findings regarding data location and ownership**

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managing meta-, macro-, and micro-adaptations (4.1)</strong></td>
<td>- TLA Processors and Data Core should operate at the appropriate level</td>
</tr>
<tr>
<td></td>
<td>- User Facing Apps may want to do their own macro- and micro-adaptation</td>
</tr>
<tr>
<td></td>
<td>- Giving apps access to TLA Data Store impacts privacy</td>
</tr>
<tr>
<td></td>
<td>- Access models for TLA may be difficult to understand</td>
</tr>
<tr>
<td></td>
<td>- Client-side methods are ideal for micro-adaptations</td>
</tr>
<tr>
<td></td>
<td>- Users are worried about loss of client-side data</td>
</tr>
<tr>
<td><strong>Data ownership and stewardship (4.2)</strong></td>
<td>- User data can be treated like a 401(k)</td>
</tr>
<tr>
<td></td>
<td>- User data can be owned by multiple entities at once</td>
</tr>
<tr>
<td></td>
<td>- A designated &quot;data steward&quot; can make decisions regarding user data</td>
</tr>
<tr>
<td></td>
<td>- Using the Two-Person Concept can prevent leaks and attacks</td>
</tr>
<tr>
<td></td>
<td>- Portable models are essential for life-long learning</td>
</tr>
</tbody>
</table>
Table 15: Recommendations regarding managing meta-, macro-, and micro-adaptations

<table>
<thead>
<tr>
<th>Implement the TLA Processors and Data Core at the Appropriate Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Should thus operate under the auspices of a trusted entity</td>
</tr>
<tr>
<td>- Support the portability of learning models</td>
</tr>
<tr>
<td>- Allow for interoperability of TLA processors through the xAPI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regulate Access of Individual Apps to the TLA Data Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Allow user facing apps to do their own macro- and micro-adaptation</td>
</tr>
<tr>
<td>- Put user access control mechanisms in place to regulate the use of the xAPI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use Client-Side Micro-Adaptation</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Use client-side mechanisms for micro-adaptations and adaptive recommendation presentations to prevent the storage of this highly sensitive information</td>
</tr>
<tr>
<td>- Use client-side data in an ephemeral manner to prevent data loss or theft</td>
</tr>
</tbody>
</table>

The TLA Processors and Data Core should operate at the appropriate level

The TLA Processors and Data Core process and store the users’ learner data and personal information, and expose the outcomes of this process (i.e. adaptations) to User Facing Apps through the xAPI [329]. This mechanism enables so-called “meta-adaptations”, which are essentially recommended learning activities that span the entire spectrum of user facing apps.

Since the TLA Processor and Data Core components deal with the lion share of data collection, distribution, and use, building trust between the user and these components is extremely important. Therefore, it would be advisable to put these components under strict control of a trusted entity, such as the user’s training department. However, implementing these
components at the departmental level may shield them from important insights that can be gained from data collected in other departments or divisions. It also makes TLA users’ mobility within the organization more cumbersome.

At the other end of the spectrum, one can imagine a situation where all TLA implementations share the same TLA Processors and Data Core. However, this would lead to performance issues [374], and it conflicts with the idea of the TLA as a specification rather than an actual infrastructure. Users may also have issues with the idea of a single entity that collects the data of all TLA users, especially after the recent hack of the Office of Personnel Management (OPM), the agency that recruits and vets prospective federal employees. In this hack, the personal information of approximately five million current and former federal employees and government contractors was stolen [112].

A good tradeoff is therefore to put these components at a level that is “low” enough for users to trust, but high enough to allow efficient mobility and user modeling synergies. Mobility problems can be further reduced through portability requirements for the Learner Profile. Moreover, to share useful learning insights, the TLA processors of different departments/divisions can be interconnected through their aAPIs.

**User Facing Apps may want to do their own macro- and micro-adaptation**

A centralized adaptation architecture may not be the best solution for macro- and micro-adaptations. Macro-adaptations are recommendations regarding learning activities *within* User Facing Apps. While these are similar in format to meta-adaptations, they may rely on logic that the provider of the app deems proprietary business information. For example, companies like Netflix consider their recommendation algorithms to be one of their most valuable business assets [110]. So, while it is entirely possible to let the TLA Processors handle this type of adaptation, it is politically inadvisable to require this structure.

Similarly, micro-adaptations depend on intimate knowledge of the learning activities, and so it is not only politically inadvisable, but also technically cumbersome to put the logic behind the context-based adaptation of every single learning activity into the TLA Processors and the TLA Data Core.

**Giving apps access to the TLA Data Store has an impact on users’ privacy**

User Facing Apps that want to do their own macro- and micro-adaptation will need more direct access to the users’ data than through the aAPI alone. Specifically, they may need access to the xAPI (for macro-adaptations) and the cAPI (for micro-adaptations). Allowing such access has an enormous impact on users’ privacy, because it moves the TLA from a situation where all user data is stored and processed by a single entity (i.e. the entity that controls the TLA processors and Data Core) to a situation where individual apps have access to the user’s data.
The TLA can deal with this situation in two different ways: On the one hand, they can provide the User Facing Apps unfettered access to the users’ data. Research has shown, though, that users are likely to trust different personalization providers to a much different extent, and that this trust can be a very personal decision (e.g. while user X may trust app A more than app B, the opposite might be true for user Y) [194]. Therefore, some sort of access control mechanism is needed to allow applications to optimally utilize the users’ data while at the same time respecting each user’s privacy preferences [18, 218].

**Access models for TLA may be difficult for users to understand**

The access control model for the TLA is potentially very difficult for users to understand. The reason for this is the complex ways in which data can be collected, stored and used by different parts of and implemented TLA architecture. Notably:

- An app that **collects** data does not **store** this data; that part is done centrally, in the TLA Data Core. This means that a (potentially less-trusted) User Facing App **mediates** the data collection practices of the (hopefully well-trusted) TLA Data Core. This may cause confusion on the users’ side, causing them to disclose less information.
- Any of the centrally stored data may be used by the TLA Processors to produce meta-adaptations. Even if the TLA Processors are well-trusted, this recombination of data may result in extremely accurate recommendations [288, 348] that may at times be perceived as “creepy”. It would be difficult for users to anticipate such potential usage of the collected data [55].
- Moreover, any app could potentially request access to any data collected by any other app, for the purpose of macro- and micro-adaptations. This kind of cross-domain adaptation is difficult to understand, and hard to regulate [47].

Given the potential abundance of data types, User Facing Apps, and connections among and between them, a typical “who gets to see what and when” access control mechanism would arguably be too complicated for most users [214, 277]. This argument, as well as potential alternatives, will be explored in Section 6. We believe that the sheer complexity of this situation may make User-Tailored Privacy the only viable solution.

**Client-side mechanisms are ideal for micro-adaptations**

In Section 2, we noted how fine-grained learner runtime data and context data can contain extremely sensitive information about the user. This type of data is typically used for micro-adaptations that occur within a single learning activity. Can we support such micro-adaptations without collecting a vast amount of sensitive data?
A technical solution that has recently become popular abandons the assumption that personal data must be sent to a remote server for adaptation to take place. Rather, this “client-side” solution enables all necessary calculations take place on the user’s own device [49, 159, 252]. Research in recommender systems shows that users prefer client-side methods as a means to alleviate privacy concerns [194, 342].

Although client-side adaptation mechanisms are typically limited in their ability to leverage data from other users, distributed and hybrid versions of collaborative filtering algorithms do exist [46, 319, 367]. Preventing anyone from accessing personal data enhances user privacy [331]. However, client-side adaptation methods can only use limited inference methods (e.g. if-then rules, simple classification) that can be executed directly on the user’s device. They also do not contribute to the TLA Data Core, although hybrid methods exist [25].

The lack of generalized learning is less problematic for micro-adaptations, because they are typically app-specific anyway. That said, transferrable insights can still be shared with other applications without having to share the data itself. An additional benefit of client-side micro-adaptations, is that they can operate even when the user is offline, such as on a plane or in remote regions with limited cellular coverage.

Users are worried about the potential loss of client-side data

Research has shown that client-side personalization is not without problems. Specifically, users are concerned that their data can be hacked if their device is stolen, and that their user model is lost forever in case they lose or break their device [195]. Micro-adaptations may however not suffer these consequences, as they are usually ephemeral: they rely only on the current learner runtime and/or context data. It is thus best to implement this mechanism without storing any of such data on the user’s device.

Recommendation: Use the TLA processors for meta-adaptations, individual apps for macro-adaptations, and client-side methods for micro-adaptations

It is impossible to provide high-quality personalized training recommendations without collecting, storing, and processing some data server-side, especially when centralized goals are expected to be taken into account in the adaptation process. A good design compromise would be a three-tier adaptation approach: On the first tier, resources, mission goals, and users’ previous learning outcomes are used by the TLA processors to decide what training applications to recommend to the user (meta-adaptation). On the second tier, individual training applications can use similar data—albeit with strictly regulated access control—to make app-level adaptations (macro-adaptation). Finally, on the third tier, client-side mechanisms can use fine-grained learner runtime data and behavioral tracking to make subtle adjustments to the learning experience (micro-adaptation). Such client-side mechanisms can also be used to decide upon the
ideal presentation and timing of the learning recommendations themselves (part of the Recommendation UI). These recommendations to ADL and other TLA performers are depicted in Figure 10, and further specified below:

- **Implement the TLA Processors and Data Core at the appropriate level**—These components deal with a large amount of potentially sensitive user data, and **should thus operate under the auspices of a trusted entity**. If this means that separate processors and data cores are needed for each department/division, then the TLA specification should support the portability of learner models and allow for interoperability of TLA processors through the aAPI.

- **Regulate access of individual apps to the TLA Data Core**—Since apps may consider their internal adaptation strategy a business asset, the TLA specification should **allow user facing apps to do their own macro- and micro-adaptation**. This requires access to the TLA Data Core, and the TLA specification should put access control mechanisms in place to regulate the use of the xAPI.

- **Use client-side micro-adaptation**—Micro-adaptations and presentation choices for the learning recommendations themselves are usually based on fine-grained learner runtime data and contextual information. The TLA can use **client-side mechanisms for micro-adaptations and adaptive recommendation presentations to prevent the storage of this highly sensitive information**. This mechanism should use client-side data in an ephemeral manner to prevent data loss or theft.

![Figure 10: Proposed Architecture with Access Control for macro-adaptations and client-side micro-adaptations.](image-url)
4.2 Data ownership and stewardship

As different entities contribute to the TLA Data Core, the collected data can be owned by multiple entities at once. To improve openness and mobility, we propose to treat users’ data like a 401(k):

- This allows users to take active ownership over their data and decisions involving their data.
- It allows this ownership to be partially shared with other contributors.
- It allows users to delegate control to a fiduciary, or “data steward”.
- It enables users to move their data from one organization (one TLA instance) to the next.

This subsection discusses the mechanisms of shared ownership, stewardship, and data mobility. Moreover, we discuss how sharing and processing decisions that involve multiple stakeholders can be implemented using the “Two-Person Concept” [365] as a means to prevent data leaks and extortion/social engineering attacks (see Table 16).

<table>
<thead>
<tr>
<th>Table 16: Recommendations regarding data ownership and stewardship</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Give Users Ownership Over Their Data</strong></td>
</tr>
<tr>
<td>- Give users the right to peruse their raw data and user models</td>
</tr>
<tr>
<td>- Structure data ownership like a 401(k)</td>
</tr>
<tr>
<td><strong>Give Employers and Apps Limited Co-Ownership</strong></td>
</tr>
<tr>
<td>- Allow employers and apps to co-own the data</td>
</tr>
<tr>
<td>- Request minimal amounts of data, avoid duplicate storage, and de-identify data</td>
</tr>
<tr>
<td><strong>Allow Users to Designate a “Data Steward”</strong></td>
</tr>
<tr>
<td>- Allow users to delegate responsibilities to a “data steward” to manage the user’s data under a strict fiduciary policy</td>
</tr>
<tr>
<td>- Implement the Two-Person Concept</td>
</tr>
<tr>
<td><strong>Make User Models Portable</strong></td>
</tr>
<tr>
<td>- Enable users to take their data with them to their new job</td>
</tr>
<tr>
<td>- Retain limited access to ex-employees’ data</td>
</tr>
<tr>
<td>- Implement Private Equality Testing</td>
</tr>
</tbody>
</table>

* A TLA user’s data can be treated like a 401(k) *

The end-user license agreement (EULA) of most modern online services claim full ownership over the personal information they collect about their users. The legality of this claim is questionable, though: the legal concept of “owning information” is still new, and laws are still being written about this topic [236, 401].

Preliminary debates and investigations among users show that there are merits in granting end users ownership over the personal information that is collected about them [302, 351]. Indeed, granting the user the right to peruse their raw data and user models is in line with TLA’s “open”
philosophy. Giving users ownership over their data also expedites the movement of data among different TLA instances—something that is very desirable given the decentralized nature of TLA and its focus on quantified self and lifelong learning [310].

Conceptually, data ownership can be structured like a 401(k): users formally own the data, but allow their employer to manage and contribute to the data. If a user moves, the data can move with them. Over time, data from different sources culminate into a well-rounded profile of the user’s certifications and other capabilities.

A TLA user’s data can be owned by multiple entities at once

Data ownership is not exclusive, and it may be desirable to give other entities partial co-ownership over the user’s data. For example, the user’s employer—who provides the user access to its TLA and the connected training applications—should also have a right over some of the data that is collected about its employee. This particularly holds true for training data itself, since it enables the company to do learning analytics, and to utilize the data in making promotion decisions. As discussed in the previous subsection, such usage may occur at a higher level in the organization, and so the user should be aware of the possibility that their data may be shared laterally within the organization for analytics and promotion purposes.

Similarly, individual training applications may use internally generated data—as well as data requested from the TLA Data Core—for macro-adaptations and internal analytics. For internally generated data, this practice mimics typical industry practices [236, 401]; for data requested from the TLA Data Core, users should be asked for permission first.

In any case, co-owners should treat user data with care. In contrast to the Big Data “collect everything mentality” [384] which permeates the current online landscape, they should request minimal amounts of data, avoid duplicate storage, and de-identify data where feasible.

A designated “data steward” can make decisions regarding TLA users’ data

Data ownership puts an important responsibility on the shoulders of users. Users can decide to play an active role in making sharing decisions about their data (e.g. “who gets to see what and when” [214, 277]), but not all users may be motivated and capable of taking on this responsibility (see Section 1.2). Expanding upon the analogy of a 401(k), the TLA user should be allowed to partially delegate the responsibility of making decisions regarding their data to a fiduciary, such as their training department manager. As a “data steward” this fiduciary is allowed to make decisions about the data on the user’s behalf.

Like with a 401(k), data stewards should adhere to a strict policy that outlines the intent behind their decisions and the limits of their powers. Such a policy may be a generic organizational policy, but it could also be created in a way that keeps each individual user’s control preferences
in mind. As such a policy can become rather complex, steps need to be taken to improve the transparency of the policy (see Section 6.1).

The fiduciary policy can outline several practices (e.g. sharing rules, processing rules) that are always allowed, never allowed, or require the explicit consent of the user. In the latter case, such consent should not just be a notice with an option to “opt out” [157, 204, 205] (Section 6.3 explains why this practice does not meet the standards of informed consent). Rather, it should ask the user to formally opt-in to the proposed practice. Another option is to combine opt-in and opt-out consent practices by algorithmically anticipating the individual user’s likely response (this is in line with the idea of User-Tailored Privacy, as discussed in Section 6.4).

**Using the Two-Person Concept can prevent leaks and attacks**

The consent procedure of the data steward’s fiduciary policy implements a Two-Person Concept solution (a concept proposed by US Air Force Instruction 91-104 [365]) that prevents any single person from intentionally or unintentionally leaking data or becoming victimized by extortion or social engineering attacks [400].

This principle also works the other way around: TLA can be implemented in such a way that the employer must give their formal approval when an employee wants to share their data with other entities pertaining to the training they did while working for that employer.

**Portable user models are essential for life-long learning**

Throughout their career, users may move between different employers, gaining experience, certifications and capabilities along the way. Figure 11 addresses the privacy of user models that are portable, i.e., that can move with the user from one employer to the next.

Different employers may use different instances of TLA. User data should therefore be specified in a standard format that allows it to be portable between TLA instances. On top of this, clear policies must be in place for when a user transfers out of their current unit [312], both in terms of what data can still be used by the former employer, as well as what data can transfer to the new employer.

In terms of the former employer, the data collected during the user’s employment should still be accessible for analytics purposes even after the user leaves. At this point, though, new updates to the user’s data should no longer be propagated to the former employer. Moreover, insofar as the former employee’s identity is not needed for analytics purposes, the data of this employee can be de-identified, and any data that does not contribute to the analytics practices could be removed.
From a practical perspective, it may be useful to “purge” the data of ex-employees with a bit of a delay, because even if they own a portable copy of their user data, it may not always be correct, and users may initially have to come back for clarifications and corrections. Moreover, users may wish to ask their employers for a letter of recommendation, which would likely be based on their training data. For requests for recommendations that happen after the data has been de-identified, users could temporarily re-grant their former employer access to their data.

Not all data may be transferred to the new employer—the user may have certain “classified capabilities” that cannot be transferred if their new employer does not have clearance to know about these capabilities. The Two-Person Concept prevents the user from accidentally disclosing classified training data to entities without clearance. Alternatively, the concept of Private Equality Testing (PET) can be used to disclose classified capabilities without leaking them [20, 92, 150]. The user themselves may also decide to redact certain information.

Figure 11: Managing privacy in portable user models
As legal aspects of data ownership are still being debated, we recommend that TLA developers proactively decide on this question in the development of the TLA protocols and service specifications. This subsection recommends a user-centric ownership model that has facilities for portability, delegation, and shared ownership. Specifically, based on the presented analysis, we can make the following recommendations:

- **Give users ownership over their data**—In the spirit of “open” learning models that support mobility and lifelong learning, TLA should give users the right to peruse their raw data and user models, e.g. by structuring data ownership like a 401(k).
- **Give employers and apps limited co-ownership**—TLA should allow employers and apps to co-own the data for narrowly specified purposes, provided that they request minimal amounts of data, avoid duplicate storage, and de-identify data where feasible.
- **Allow users to designate a “data steward”**—TLA managers should allow users to delegate responsibilities to a “data steward”, such as their training department manager. This data steward should manage the user’s data under a strict fiduciary policy, that might be tailored to the user’s privacy preferences. To keep users in the loop, and to prevent leaks and attacks, important decisions should implement the Two-Person Concept, where both involved parties have to authorize new data practices.
- **Make user models portable**—As users move between employers, TLA should enable users to take their data with them to their new job. The former employer may retain limited access to ex-employees’ data for analytical purposes. The TLA can implement Private Equality Testing to disclose classified capabilities to authorized parties without leaking them.
5 Data sharing

Problem: How can data be shared with people and organizations? The previous section covered the exchange of user data between TLA-based applications. Data collected in the TLA Data Core can however also be used by people and organizations. What are the consequences of such social data sharing?

Current state of the art: Privacy implications of social and organizational data use are unknown. The TLA specifications call for an Open Social Learner Model (OSLM) that allows learning materials, activities, and outcomes to be shared across learners (enabling peer interactions) [370]. Moreover, the TLA design rationale puts a lot of emphasis on learning research [310, 329]. Finally, the collected TLA data can be used to make mission planning and promotion decisions. The consequences of these applications of data collected by TLA-based systems are however currently unknown.

Solution: Study the consequences of the social and organizational use of data in TLA-based systems. This section covers how recipients may use user data for various purposes while keeping the user’s privacy in mind. We make the following observations:

- Sharing data with the users themselves increases trust, and can enable powerful “quantified self” experiences.
- Some user data may be shared with other users to create social learning experiences. The FERPA laws must be respected here, and care must be taken to create social learning experiences that are meaningful and not overwhelming or discouraging.
- Employers can use data about their employees to do research, and make mission planning and promotion decisions. Employers should carefully adhere to laws and regulations that protect users from unethical treatment.

Key findings and recommendations are presented in Table 17.
Table 17: Key findings regarding data sharing

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrutability and the quantified self (5.1)</td>
<td>Scrutable Profiles increase trust and quality</td>
</tr>
<tr>
<td></td>
<td>Promoting the quantified self turns users into active learners</td>
</tr>
<tr>
<td>Social learning experiences (5.2)</td>
<td>FERPA prevents disclosure of educational records</td>
</tr>
<tr>
<td></td>
<td>Users may fear &quot;social overload&quot;</td>
</tr>
<tr>
<td></td>
<td>Communication styles and social comparison styles influence social dynamics</td>
</tr>
<tr>
<td></td>
<td>Peer assessment depends on social dynamics</td>
</tr>
<tr>
<td>Research, promotion, and mission planning (5.3)</td>
<td>IRBs require anonymized data</td>
</tr>
<tr>
<td></td>
<td>For placement, competency and preferences may be at odds</td>
</tr>
<tr>
<td></td>
<td>Algorithmic promotion decisions could obscure unwanted biases</td>
</tr>
</tbody>
</table>

5.1 Scrutability and the quantified self

The first and foremost entity with whom TLA can share its data is the user themselves. In this subsection, we argue that giving users insight into their user model can increase their trust, and even empower them to become more active learners (see Table 18).

Table 18: Recommendations regarding scrutability and the quantified self

<table>
<thead>
<tr>
<th>Implement Scrutability</th>
<th>Leverage TLA for the Quantified Self</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to inspect and correct their profiles</td>
<td>Use the quantified self as a motivator for data collection</td>
</tr>
<tr>
<td>Use the quantified self as a motivator for data collection</td>
<td>Turn users into active learners using compelling infographics that establish unique behavioral connections</td>
</tr>
<tr>
<td>Turn users into active learners using compelling infographics that establish unique behavioral connections</td>
<td>Use gaming elements to enable users to push themselves further</td>
</tr>
<tr>
<td>Use gaming elements to enable users to push themselves further</td>
<td>Avoid turning the quantified self features into a source of unwanted pressure</td>
</tr>
</tbody>
</table>

TLA’s Learner Profiles are based on advanced analysis of user behavior by the TLA Processors. The results of this analysis may not always be intuitively understandable to the user. Moreover, in some cases the insights or the facts on which they are based are incorrect, and it may be difficult for users to correct such mistakes. Building the Learner Profiles in line with the principles of “scrutability” makes them easier for users to understand and correct.
Several researchers have argued that explanations and control are important qualities of an intelligent system:

- Höök et al. were among the first to suggest a “glass box” model for adaptive hypermedia systems [140].
- Tintarev and Masthoff suggest to “explain how the system works” and to “allow users to tell the system it is wrong” [353, 354].
- Kay and Lum further unpack the idea of providing explanations, suggesting to explain why individual elements and relations in the underlying model have particular values [164].

Some researchers have shown that providing explanations and control indeed improves users’ understanding:

- Herlocker argues that “exposing the reasoning behind a recommendation” provides transparency [133] (see also [73, 74]).
- Tintarev and Masthoff show that explanations make it easier to judge the quality of recommendations [355].
- Sinha and Swearingen demonstrate that users rate systems that provide detailed information about items as more useful and easier to use [323] (see also [114]).
- Knijnenburg et al. show that mechanisms that increase transparency and control both contribute to the perceived recommendation quality and users’ satisfaction with the system [177].

Finally, research shows that explanations and control increase trust:

- Cramer et al. and Felfernig argue that explanations increase users’ trust in the recommendations [66, 96].
- Guy et al. and Wang and Benbasat show that explanations increase the perceived competence of a system [120, 373].
- Finally, Knijnenburg demonstrates that users’ understandability of and control over the personalization process influence their perceived trust and privacy threat [175].

Implementations of “scrutability” in learner models can take several levels of complexity, but it is best for the user to keep things simple. An example of a very simple scrutinable user model is Google’s Ad Personalization page (Figure 12). This page shows the topics that Google has derived the user is interested in. It allows users to see how these insights were generated (“Where did these come from?”), and gives users the option to add or remove individual topics.
Taking scrutability to a higher level, the learner modeling insights can be used to create a “quantified self” experience. The quantified self is a movement of users tracking information about themselves and using it to form insights for self-improvement. A good quantified self experience makes it easy to get data about everyday activities without having to consciously think about the process of data acquisition [215]. As mentioned in the TLA design rationale, the TLA could help individuals learn about themselves by facilitating the empirical measurement and manipulation of individual experience [310]. This way, TLA-based systems can help the user to improve their lifestyle.

Since the quantified self experience helps users to improve themselves, it is a reason for many people to accept the potential privacy intrusion that comes with wearable technology and constant tracking [26, 121]. As such, the quantified self can be a motivating factor behind TLA’s data collection efforts.

Similarly, the quantified self can turn users into “active learners” through a process of self-actualization [188]. At a general level, the developers of some commercial recommender
systems (e.g. OkCupid, The EchoNest\textsuperscript{3}) have recently started to share fascinating insights into consumer tastes on their company blogs. These analyses often use compelling infographics to highlight surprising preference dynamics, sometimes broken down by state, gender, age or other demographic dimensions. Could such analyses be personalized? This would allow users to gain insights from patterns in their behavior that show a previously unknown connection (e.g. “I seem to get tired when my carbohydrate consumption is high... maybe my eating behavior causes my sleepiness”). Carefully constructed personalized infographics can allow users to explore the common and unique sides of their identity, and—if comparable across users—provide a starting point for establishing sub-cultures with similar abilities and limitations that they can explore or exploit together (see Section 5.2).

Finally, the quantified self can be a catalyst for learning. Translating self-tracked parameters into a game-like structure can create new motivational and pedagogical support structures that encourage and enable users to push themselves further [63, 107]. Games can be addictive, though [284, 334], and a system that urges the user for perfection and constantly pushes their boundaries could become a source of unwanted pressure on the individual to perform [372].

### Recommendations: Implement scrutability, and leverage TLA for the quantified self

Sharing TLA Learner Profile info with the users themselves can keep them in the loop, help them understand the system, and increase trust. By presenting connections between data dimensions, TLA-based systems can turn users into active learners. Based on the presented analysis, we can make the following recommendations:

- **Implement scrutability**—TLA’s Learner Profiles are based on complex inferences. The TLA Data Core should therefore have facilities to allow users to inspect and correct their profiles as needed. Scrutability increases users’ understanding of the recommendation process, and is instrumental in building trust.

- **Leverage TLA for the quantified self**—Learner Profiles are an excellent source of information for the user to gain insights about themselves. As such, TLA can use the quantified self as a motivator for data collection. This paradigm can turn users into active learners using compelling infographics that establish unique behavioral connections. Moreover, TLA could use gaming elements to enable users to push themselves further. However, TLA should avoid turning the quantified self features into a source of unwanted pressure.

\textsuperscript{3} http://blog.okcupid.com, http://blog.echonest.com
5.2 Social learning experiences

Research suggests that cooperative learning improves learning performance [156], even when it occurs in a computer-mediated fashion [166]. Communication, coordination, and collaboration can help learners support each other and improve themselves. Even competition [156] may result in cooperative benefits when implemented in a careful manner. TLA specification-enabled learning applications can provide a digital environment to support these benefits of cooperative learning.

That said, cooperative learning can also result in privacy problems: the social learning environment may disproportionately promote certain personalities and communication styles, may overload users, and may result in unfriendly interactions. This subsection addresses these privacy concerns as well as potential mitigations. We make suggestions for networking facilities that promote inclusion, foster healthy social dynamics, and limit social overload (see Table 19).

Table 19: Recommendations regarding social learning experiences

<table>
<thead>
<tr>
<th>Give Users Control Over What to Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Refrain from sharing any learning outcomes with others by default</td>
</tr>
<tr>
<td>- Require an explicit decision from users before sharing learning outcomes with others</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Users to Limit Their Social Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Allow users to limit their connections to those they deem relevant for each application</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implement a “Learning Buddy” Recommender</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Pair learners with similar communication styles</td>
</tr>
<tr>
<td>- Pair learners with compatible social comparison styles</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Involve Users in the Determination of the Peer Evaluation Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Peer evaluations that are simple and allow for feedback</td>
</tr>
<tr>
<td>- Create a cooperative culture around peer evaluation</td>
</tr>
<tr>
<td>- Determining the peer evaluation procedures by consensus</td>
</tr>
</tbody>
</table>

**FERPA prevents TLA from disclosing educational records**

Enterprise social networking research shows that social networking helps to establish social norms [368], foster connections [268], and catalyze innovation [216, 217] among employees. These benefits seem to extend to learning as well: A study conducted at National Central University shows that learners are interested in seeing who is online and messaging them when they want to [399]. Among other things, status awareness can help with participation [93] and social navigation [94].

Note that sharing the user’s current learning status can in some cases be considered a violation of Family Educational Rights and Privacy Act (FERPA) and state laws, which prevent educational institutions from disclosing educational records to the public. Care should thus be taken that the user (not the system) makes the decision to disclose such information.
How should social networks within a TLA-based learning environment be established? One possibility is to leverage users’ existing social networks. A problem with this implementation is that users may not consider all their existing social connections to be “close friends”—users of e.g. Facebook have a median of 200 contacts [1] and average seven new contacts a month [124]. If all these connections are shared with learning applications to create social learning experiences, users may rightfully fear that they could become bothered by an overload of social activity [270]. As a potential protection mechanism, we suggest that the TLA allows users to limit the sharing of social network connections to only those connections that the user deems relevant for each specific learning application.

Communication styles and social comparison styles influence social learning dynamics

Beyond allowing users to restrict their interactions to a limited number of connections, the TLA processors can also play an active role in helping users to select an appropriate learning community. This model can prevent the community from becoming unbalanced in a way that can lead to a skewed contribution model. The discussion boards of MOOCs, for example, seem to have problems with a large number of “lurkers” that may post questions but never answer them [38, 134, 201], while enterprise social networks occasionally show the opposite problem of excessive contributors that do not consume the produced content of others [269]. A careful mix of consumers and contributors prevents a social learning network from becoming ineffective.

Communication style can be another criterion for learning community selection. Moreover, the communication mechanisms provided to the network can be tailored to the predominant communication style. Referring to Section 1.3, it is important to note that messaging facilities are a typical non-FYI communication solution, while status awareness fits with FYI communicators. So conversely, the status awareness functionality may not be suitable for non-FYI communicators, and the direct messaging functionality may eventually irritate FYI communicators [270]. A possible solution, then, would be to build social learning system in a way that not only supports different learning styles [117], but also different communication styles [273].

Another thing to consider is the social dynamic involved in the creation of pairs or groups of learners. From a privacy perspective, it is better not to let everyone compare themselves against everyone else: this is overwhelming and likely ineffective. Rather, social psychology tells us that people engage in social comparison processes when they feel uncertain about their performance [138], and that some prefer to engage in upward social comparison (comparing themselves against aspirational peers), while others prefer to engage in downward social comparison
(comparing themselves against trailing peers) [346]. Therefore, pairs of one upwards comparator and one downwards comparator may result in the most ideal social dynamic.

Peer assessment and social dynamics

Peer assessment is formative feedback that will help and motivate users to perform better. A socially-capable TLA specification-based implementation can provide ample opportunity for peer evaluation. To limit intrusion into the time of the evaluator, it is necessary that peer assessment methods are easy to understand and do not take too much time [340]. To be fair to the person being evaluated, it is important to allow them to reply to the evaluation [118] (see Section 2.2).

Another question is whether peer evaluation should be anonymous or not. Research suggests that the accuracy and trustworthiness of the assessment will be higher for anonymous peer reviews [161]. Without anonymity, users may feel uncomfortable giving an honest evaluation. This is even more true when evaluations include not just performance but also value perspectives [161].

In small groups peer anonymity is hard to ascertain, as social processes outside the review procedure may easily reveal the identity of the evaluators. Moreover, weak evaluations may result in mistrust, and in high-stakes team situations (e.g. a military unit), openness may be the only way to prevent criticism from ruining the social dynamic. A possible solution is thus to involve users in the determination of the peer evaluation procedures [161]; this will guarantee that users will find these procedures acceptable and fair.

The effect of peer assessment may depend on the social dynamic of the online interaction. Gamification (mentioned earlier) can enable users to push themselves further [63, 107], but when used in a social environment, it can also turn into a competitive dynamic. This dynamic can be good or bad, depending on how it is implemented.

Recommendation: Create a selective social learning environment with a positive group dynamic

A TLA implementation with a social component can have a very beneficial impact on learning outcomes, but it can also result in social overload. Interaction can be beneficial, but differences in communication styles can result in friction, as can incompatible social comparison styles. At a more formal level, peer assessment may have a positive or a negative impact, depending on the social dynamic that the system creates (competitive or cooperative). Based on the presented analysis, we can make the following recommendations:

- **Give users control over what to share**—FERPA prevents TLA from disclosing educational records to the public. In case of social sharing, TLA should thus refrain from sharing any
learning outcomes with others by default. Rather, TLA should require an explicit decision from users before sharing learning outcomes with others.

- **Allow users to limit their social connections**—Users may not want to share their learning experience with all their social network contacts. Instead, a socially-capable TLA experience should allow users to limit their connections to those they deem relevant for each specific learning application. This prevents social overload.

- **Implement a “learning buddy” recommender**—To support users in selecting the best social connections to include in their learning experience, a socially-capable TLA should implement a recommender that can pair learners with similar communication styles to prevent unbalanced contributions. That recommendation can also pair learners with compatible social comparison styles, specifically, a person who prefers upward social comparison should be paired with a person who prefers downward social comparison.

- **Involve users in the determination of the peer evaluation procedures**—An important aspect of a socially-capable TLA environment is that it allows for mutual assessment. Users should have access to peer evaluations that are simple and allow for feedback. To prevent criticism from ruining the social dynamic, it is better to create a cooperative culture around peer evaluation. Training department managers can accomplish this by determining the peer evaluation procedures by consensus.

### 5.3 Research, promotion, and mission planning

The primary purpose of data collected by TLA-based systems is to allow the TLA Processors to provide personalized learning recommendations. The data can however also be used for research, for mission planning, and to decide on promotions. Privacy experts argue that secondary use of information should be explicitly communicated to the users, otherwise they may be surprised to find out about it, and feel that their privacy is violated [347].

The use of data for research, promotion, and mission planning is particularly sensitive because it involves employers collecting and using data about their workers. Researches have shown that “on the job monitoring/tracking” can have a deleterious effect on workers’ performance. Specifically, whereas Nebeker and Tatum show that automated computer monitoring can lead to increased speed of work, they found no improvement in work quality, satisfaction, and stress [255]. Chalykoff and Kochan in fact showed that there are significant negative effects of monitoring [53]. They were able to resolve these negative effects for some (but not all) employees by giving them extensive feedback and performance appraisal.

Aside from that, there are laws and regulations surrounding research and employment-related practices that need to be adhered to, and even beyond these formal restrictions it would serve TLA developers to think about how TLA can safeguard the ethical treatment of research subjects and employees. This subsection discusses ethical guidelines that serve this purpose.

This subsection covers the use of data for research, promotion, and mission planning (see Table Table 20). We argue for the establishment of responsible practices regarding how data will be used for these purposes, as well as the clear communication of these practices to users.
Table 20: Recommendations regarding research, promotion, and mission planning

<table>
<thead>
<tr>
<th>Let Users Know About Secondary Data Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Communicate secondary data use practices to users</td>
</tr>
<tr>
<td>– Indicate exactly which data was used and for what purpose</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Follow IRB Guidelines for Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Anonymize research data</td>
</tr>
<tr>
<td>– Allow for the communication of incidental findings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act Responsibly Regarding Placement and Promotion Decisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Establish guidelines surrounding conflicts between competence and preferences</td>
</tr>
<tr>
<td>– Make sure that promotion decisions are made in a non-discriminatory manner</td>
</tr>
</tbody>
</table>

**IRBs require research to be conducted on anonymized data**

Data captured and generated by the TLA for research purposes, allowing product developers and publishers to fine-tune their training experiences, as well as allowing education and training organizations to develop more accurate and fine-grained competency frameworks [310]. IRBs usually prefer such research to be conducted using de-identified data. However, in the era of powerful data analytics that can uncover very fine-grained insights, this raises its own ethical concerns. For example, in an analysis of big data ethics in the military, Schneider et al. ask themselves what if an analyst discovers a pattern of mental illness or suicidal thoughts in the data of a single user: “Does the military’s prerogative to prevent suicides—arguably at any cost—override [...] concerns about privacy and fairness?” [312].

Whether to report “incidental findings” to the user has been debated by ethicists, but there is no clear guidance on whether and how such findings should be disclosed [167]. As for how: one could keep a table linking participants to anonymized codes in a separate, protected location. This allows researchers to reach out to participants if an incidental finding indeed does occur.

**For placement, competency and preferences may be at odds**

TLA data can also be used to make deployment decisions, allowing supervisors to recruit teams with uniquely matched competencies, or, alternatively, train up existing teams to attain the competencies needed for a certain mission. Again, an ethical discussion would need to take place regarding the potentially conflicting roles of competency and user preferences: if a user is the only one in their division to have a certain language competency, but does not want to be deployed to the country where that language is spoken, should the user’s competency or their preference take precedence in a planning officer’s decision of whether to deploy the user? What if this decision not only affects the user, but also the rest of their unit?

As such decisions are likely going to depend on a complicated mix of factors, it is important that the procedures are supported by all employees involved. This means establishing and
communicating the procedures beforehand, and possibly giving users a say in the development of these procedures.

Algorithmic promotion decisions could obscure unwanted biases

Finally, TLA data can be used to make promotion decisions. Schneider et al. highlight the important ethical considerations of using machine judgment for promotion decisions [312]. On the one hand, one may argue that data-driven promotion decisions are void of emotional and political biases, thereby increasing fairness. On the other hand, algorithmic decisions have been shown to incorporate biases themselves—and even worse, to obscure them [229]. One may also argue that it is important not to see a user as merely the sum of his/her competencies, as some qualities may be hard to quantify.

In the context of employment discrimination laws (Title VII, ADA, ADEA), it is advisable to check algorithmic promotion and placement decisions for inadvertent discriminatory biases. This can be done by hand, e.g. using the Delphi method [303], but automated solutions may be available: recent work has explored the use of “propensity scoring” to reduce availability biases in datasets [311]. Using the same method as a post hoc filtering technique can reduce unwanted biases in recommendation results as well.

Recommendation: Start discussing the ethics of learning data analytics

Beyond existing laws and regulations, TLA developers should start discussing the ethics of learning data analytics in the context of research, promotion, and mission planning [312]. Based on the presented analysis, we can make the following recommendations:

- **Let users know about secondary data use**—Users may not expect that their data will be used for research, placement, and promotion decisions. Training department managers should communicate secondary data use practices to users. Since the TLA Data Core may contain a very wide variety of information, it is best to indicate exactly which data was used and for what purpose, and give users extensive performance appraisal.

- **Follow IRB guidelines for research**—Human subjects research is subject to review by an Institutional Review Board. IRBs usually require researchers to anonymize data as much as possible, but they allow researchers to keep a key list with research subjects’ identities in an offline secure location to allow for the communication of incidental findings.

- **Act responsibly regarding placement and promotion decisions**—Training department managers should acknowledge the fact that TLA users are more than the sum of their training data. They must establish clear guidelines surrounding potential conflicts between competences and preferences when it comes to placement decisions. Moreover, they should make sure that algorithmic promotion decisions are made in a non-discriminatory manner.
6 Privacy support mechanisms

Problem: How can we support TLA users making privacy settings? Throughout this document we have demonstrated that TLA-based systems must deal with a lot of privacy-related issues. Even when they are designed and implemented with privacy in mind, it will be inevitable for these systems to have a wide array of privacy settings that allow users to customize their experience to fit their personal preferences when it comes to the unavoidable tradeoff between privacy and utility. How can we help users in making these privacy settings?

Current state of the art: There are problems with the current paradigms of “notice and control” and “privacy nudging”. To help users with this tradeoff, many privacy experts recommend the practice of notice and control: giving users comprehensive control over their privacy, while at the same time providing them with more information about the implications of their decisions [43, 52, 213, 305, 345, 397]. Notice and control are also at the heart of existing or planned regulatory schemes [90, 381]. However, research in the past few years has unveiled a fair number of “privacy paradoxes”: situations or conditions in which transparency and control do not increase people’s privacy, or even decrease it (see Section 1.1).

An alternative solution that has recently gained more traction is privacy nudging, an approach to privacy support that attempts to relieve some of the burden of privacy decision-making, by making it easier for people to make the right choice, without limiting their ability to choose freely [4, 8, 23, 375, 376]. Privacy nudging has also had only limited success, arguably because privacy nudges take a “one-size-fits-all” approach to privacy [336]: They assume that the “right” privacy decision is the same for every user, piece of information, and situation.

Solution: Introduce personalized privacy decision support with “user-tailored privacy”. To overcome these shortcomings of transparency-and-control and privacy nudges, privacy scholars need to move beyond the “one-size-fits-all” approach that is embodied in both nudges and transparency and control. Because of the high variability and context-dependency of people’s privacy decisions, nudges need to be tailored to the user and her context. The idea of user-tailored privacy is the latest development in the quest for more usable privacy support.

This section discusses existing techniques for privacy notices, control, and nudging. It also discusses their shortcomings. It then sets the stage for user-tailored privacy, which will be central to the next version (0.2) of this specification document. Key findings and recommendations are presented in Table 21.
6.1 Privacy notices

Several designs solutions have been proposed to increase users’ understanding of privacy-related information. This subsection covers these solutions, such as nutrition labels, textured notices, and comics, and critically appraises their effectiveness (see Table 22).

<table>
<thead>
<tr>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy notices (6.1)</td>
<td></td>
</tr>
<tr>
<td>– Privacy nutrition labels give quick overview information</td>
<td>– Use textured, comic-based privacy nutrition labels</td>
</tr>
<tr>
<td>– Textured agreements connect overview to detail</td>
<td>– Choose simplicity over notices</td>
</tr>
<tr>
<td>– Privacy comics can increase efficacy and motivation</td>
<td></td>
</tr>
<tr>
<td>– Privacy notices may not always work</td>
<td></td>
</tr>
<tr>
<td>Control mechanisms (6.2)</td>
<td></td>
</tr>
<tr>
<td>– Accessible privacy controls increase self-efficacy</td>
<td>– Use accessible, graphical privacy controls</td>
</tr>
<tr>
<td>– Graphical designs can simplify access control matrices</td>
<td>– Choose simplicity over control</td>
</tr>
<tr>
<td>– Privacy control goes beyond disclosure</td>
<td></td>
</tr>
<tr>
<td>– Users are not always motivated to take control</td>
<td></td>
</tr>
<tr>
<td>Privacy nudging (6.3)</td>
<td></td>
</tr>
<tr>
<td>– Justifications provide a shortcut to decision-making</td>
<td>– Use nudges if there is a virtual consensus</td>
</tr>
<tr>
<td>– Audience feedback makes users more aware of who sees their data</td>
<td></td>
</tr>
<tr>
<td>– Defaults make it convenient to take the right action</td>
<td></td>
</tr>
<tr>
<td>– Nudges may threaten autonomy</td>
<td></td>
</tr>
<tr>
<td>User-tailored privacy (6.4)</td>
<td></td>
</tr>
<tr>
<td>– Privacy behaviors vary, but are predictable</td>
<td>– Employ user-tailored privacy when possible</td>
</tr>
<tr>
<td>– Users’ behaviors can be used to make adaptations</td>
<td></td>
</tr>
</tbody>
</table>

Table 21: Key findings regarding data sharing

Table 22: Recommendations regarding privacy notices

**Use Textured, Comic-Based Privacy Nutrition Labels**

– Use privacy nutrition labels to give people a quick overview
– Make privacy notices textured to connect to the details
– Use comics to make privacy notices attractive and approachable

**Choose Simplicity Over Notices**

– Use notices sparingly
– Make privacy decisions simpler rather than relying on notices

“Privacy nutrition labels” give quick overview information

One realization about privacy notices is that the complexity of online privacy policies is ever-increasing [245]: they are often written in a legalistic and confusing manner, and require a college reading level to understand them [16, 50, 171, 238, 363]. Indeed, while many people claim to read online privacy policies [147, 244], many do not actually read them [9, 30, 31, 129, 154, 171, 322, 362], or do not read closely enough to understand them [274]. A lot of work has therefore gone into standardizing and summarizing privacy statements [111].
A problem with summarizing privacy notices is that they are often too simplistic to accurately represent the policies they reflect [258]. If users ignore the full policy, they may thus not have all the information they need to make a decision [165].

Textured agreements keep the original policy intact, but add layers of emphasis (e.g. headings, bullets, bold text, highlights, graphics) to make the text more readable [165, 350]. Textured agreements increase (rather than decrease) the amount of time people spend reading the agreements, primarily because more participants end up looking through the entire agreement.

Another design idea used to increase users’ efficacy and motivation to read privacy policies is to use comics. Comic books are already used to e.g. increase literacy [42, 102] and provide health education [113, 235]. The visual aspects of comics are captivating, and can often be used to understand the story without having to read any text [86, 165]. This makes them particularly appropriate for increasing the motivation and self-efficacy of people with lower literacy levels and/or a visual learning style [85, 297]. Work on privacy comics is still in its infancy [178], but we argue that they are likely to be uniquely capable of instilling motivation and ability in users, who would normally forgo learning about privacy.

Although the consensus is that users should be informed about the privacy decisions they are asked to make [87, 145, 243, 301, 396], the reality is that doing so often makes users more fearful or unwilling to come to a decision. For example:

- Marketers have discovered that displaying a privacy label on an e-commerce website—a supposed vote of confidence in the site’s privacy practices—may decrease instead of increase purchases [2, 33, 142].
- Privacy policies have been shown to incite privacy concerns rather than easing them [291].
- John et al. [155] demonstrate that even subtle privacy-minded designs and information may trigger users’ privacy fears and thereby reduce disclosure and participation rather than increasing it.
- Adjerid et al. [8] show that the impact of privacy notices depends on their specific framing, and that distractions can easily nullify any effect of privacy notices.
The conclusion, then, is that transparency does not work well in practice, especially for systems that process large amounts of personal data, which is increasingly the case online [352]. Nissenbaum [258] postulates this as the Transparency Paradox: privacy notices that are sufficiently detailed to have an impact on people’s privacy decisions are often too long, detailed and complex for people to read.

**Recommendation**: Where appropriate, use textured, comic-based privacy nutrition labels

TLA-based implementations are likely to have a plethora of privacy settings. Users should not be expected to understand these settings without help. Based on the presented analysis, we can make the following recommendations to ADL and other TLA performers:

- **Use textured, comic-based privacy nutrition labels**—Users are likely not going to read full-length privacy statements. User-facing apps should therefore use privacy nutrition labels to give people a quick overview of the privacy implications of using the system. An overview is likely not enough to help users make fully informed decisions, hence applications should make privacy notices textured to connect to the details of the available privacy settings. Finally, applications should use comics to make privacy notices attractive and approachable to people at lower reading levels.

- **Choose simplicity over notices**—Privacy notices sometimes have an effect that is opposite from the intended effect. Hence, TLA-based applications should use notices sparingly, and work to make privacy decisions simpler rather than relying on notices to inform users about the decisions they are expected to make.

### 6.2 Control mechanisms

Like with privacy notices, several designs solutions have been proposed to give users more intuitive control over their privacy settings. This subsection covers these solutions—e.g., controls that are easily accessible, graphical, and go beyond information access—and critically appraises their effectiveness (see Table 23).

**Table 23: Recommendations regarding control mechanisms**

<table>
<thead>
<tr>
<th>Use Accessible, Graphical Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make controls obvious and easily accessible</td>
</tr>
<tr>
<td>Use graphical methods to provide control</td>
</tr>
<tr>
<td>Provide controls that go beyond information access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Choose Simplicity Over Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a privacy setting that works for everyone (where possible)</td>
</tr>
<tr>
<td>Not make control too detailed</td>
</tr>
</tbody>
</table>
Knijnenburg et al. investigated form auto-completion tools, which automatically fill out Web forms based on previously collected personal information [183]. They demonstrated that users of these tools typically fail to consider the perceived risk and relevance of each piece of potentially private information. Consequently, they developed two alternative design solutions to promote more explicit privacy decision making. The first design solution—the “remove” type auto-completion tool—improves upon traditional auto-completion by allowing users to remove an auto-completed entry by means of a button adjacent to each field. The second design solution—the “add” type auto-completion tool—leaves all fields blank by default and provides a button to add the pre-collected information to each field. Knijnenburg et al. argued that the process of disclosing personal information is more elaborate for users of the add/remove auto-completion tools than for users of the traditional auto-complete tool. In their experiment, they indeed demonstrate that due to the availability of buttons, users feel more able to take control over their disclosure, and hence become more deliberate about their decisions when using add/remove tools.

These results suggest that simple privacy controls can make users feel more in control—and, indeed, take control—over their privacy-settings. Even though the suggested buttons made removing/adding information only slightly easier, they significantly increased users’ focus on the purpose of the requested information in deciding what to disclose.

In many cases, privacy control can be formulated as an “access control matrix”, for example when deciding what to share with whom. Such a control matrix may for example be required to specify which User Facing Apps have access to what data in the TLA Data Core (see Section 4.1).

Several solutions have been proposed to simplify such control matrices. One solution is to group recipients, cf. “Circles” in Google+ [160, 181, 377]. Another solution involves creating a graphical representation of the control matrix that is automatically sorted to show interesting patterns [257]. Finally, Raber et al. proposed “wedges” to combine two dimensions (recipient type and social distance) in a single intuitive interface. They found that users could make more accurate privacy decisions using the wedges-based interface, and liked the interface better [295].

Selective information sharing is just one of many strategies SNS users may employ to alleviate privacy tensions [206, 233, 360]. This realization is in line with Altman’s broader definition of
privacy as “an interpersonal boundary process by which a person or group regulates interaction with others,” by altering the degree of openness of the self to others [12].

Likewise, privacy control can be provided in more diverse and more intuitive ways than a traditional “sharing matrix” in which users specify who gets to see what [136, 207, 251]. For example, Facebook’s privacy features support a variety privacy management behaviors that go beyond selective information sharing; users can also manage their privacy in terms of relational boundaries (e.g. friending and unfriending), territorial boundaries (e.g., untagging or deleting unwanted posts by others), network boundaries (e.g. hiding one’s friend list from others), and interactional boundaries (e.g. blocking other users or hiding one’s online status to avoid unwanted chats) [162, 387]. Research has found that it is important to give users the privacy features they want, lest they experience reduced social connectedness, and miss out on social capital [388].

Users may not always be motivated to take control over their privacy

The Control Paradox states that while users claim to want full control over their data [5, 28, 39, 198, 343, 344, 356, 378, 393], they avoid the hassle of actually exploiting this control [61]. In combination with overly permissive defaults [37, 116], this leads to a predominance of over-sharing. For example:

- Larose and Rifon [210] find that privacy seals influence disclosure tendencies only for participants that are either motivated or have a high self-efficacy.
- Besmer et al. [32] find that participants were only influenced by social navigation cues if they already had a tendency to change their settings.
- Gross and Acquisti [116] show that only a small number of Facebook users change the default privacy preferences.

Like transparency, control does not work well in practice. Systems like Facebook that manage large amounts of personal user data have to resort to “labyrinthian” privacy controls [91]. As a result most Facebook users do not seem to know the implications of their own privacy settings [225, 339], and share postings in a manner that is often inconsistent with their own disclosure intentions [231].

**Recommendation: Where appropriate, use accessible, graphical privacy controls**

TLA-based implementations should have privacy settings interfaces that are easy to use. Based on the presented analysis, we can make the following recommendations to ADL and other TLA performers:
• **Use accessible, graphical privacy controls**—Privacy settings should not be buried deep inside a system’s settings. Instead, TLA-based applications should make controls obvious and easily accessible. Doing so increases users’ self-efficacy. Moreover, some privacy control features can be very complex. Apps should use graphical methods to provide control in these cases; this makes control more intuitive. Finally, TLA-based applications should make sure to provide controls that go beyond information access. This allows users to address relational, territorial, network, and interactional boundaries.

• **Choose simplicity over control**—Users say they want control over their privacy, but they rarely use it. Therefore, where possible, User Facing Apps should use a privacy setting that works for everyone (where possible), so that control is not needed. In any case, apps should not make control too detailed, that way users will not feel overwhelmed.

### 6.3 Privacy nudging

*Privacy nudging*, a recent approach to support privacy decisions, tries to overcome some of the problems with privacy notices and control. Nudges are subtle yet persuasive cues that makes people more likely to decide in one direction or the other [349]. Carefully designed nudges make it easier for people to make the right choice, without limiting their ability to choose freely. This subsection describes privacy nudges that have been tested (e.g., justifications, audience feedback, and defaults), and discusses their shortcomings (see Table 24).

<table>
<thead>
<tr>
<th>Table 24: Recommendations regarding privacy nudging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Nudges if There is a Virtual Consensus</td>
</tr>
<tr>
<td>− Use justifications, audience feedback, and defaults when virtually all users agree on the optimal privacy setting</td>
</tr>
<tr>
<td>− Use nudges to provide users choice in the unlikely event that they want a different setting after all</td>
</tr>
</tbody>
</table>

**Justifications provide a shortcut to privacy decision-making**

The type of nudge that is most extensively implemented in real systems is *justifications*. A justification is a succinct reason to disclose or not disclose a certain piece of information. It differs from a privacy notice in its brevity and its purpose: rather than educating users about privacy, justifications make it easier to rationalize the decision [34, 321] and to minimize the regret associated with choosing the wrong option [62, 146]. Justifications include providing a reason for requesting the information [64], highlighting the benefits of disclosure [197, 373], and appealing to the social norm [7, 32, 278].

The effect of justifications seems to vary. Specifically:

• In a study by Kobsa and Teltzrow [197], users were about 8.3% more likely to disclose information when they knew the benefits of disclosing the information.
• In an experiment by Acquisti et al. [7], users were about 27% more likely to do disclose information when they learned that many others decided to disclose the same information.
• Besmer et al. [32] found that social cues have barely any effect on users’ Facebook privacy settings: only the small subset of users who take the time to customize their settings may be influenced by strong negative social cues.
• Patil et al. [278] rate social navigation cues as a secondary effect.
• Knijnenburg and Kobsa [182] test various different notifications, and find that while they all seem to be perceived as useful (except for the social justification), none of them seem to increase users’ trust in or satisfaction with the system.

Another justification strategy is to provide a symbolic rather than textual privacy indicator, e.g. a “privacy seal”. Again, such indicators have varied success:

• Egelman et al. [87] show that privacy indicators next to search results can entice users to pay a premium to vendors with higher privacy scores.
• Users of Xu et al.’s [396] location-based coupon service were more likely to disclose information when the site displayed either a TRUSTe seal or a legal statement.
• In Hui et al.’s [145] marketing survey, a privacy seal did not significantly increase disclosure.
• Studying an online CD retailer, Metzger [243] found that their seal had no effect.
• Rifon and Larose [301] show that warnings and seals at an online retailer website influence users in certain situations only.

Audience feedback makes users more aware of who sees their data

In social media, nudges often relate to the real or potential audience of a shared piece of information. Again, the effects of these nudges are mixed. For example:

• In location sharing services, researchers have experimented with giving users real-time feedback on who is requesting or viewing their location [153, 359]. Users appreciate the information, but find that it can easily become excessive and annoying.
• Wang et al. [375, 376] provide users with detailed feedback about the potential audience when posting a Facebook message. Some users consider this tool helpful, but they find no significant differences in posting behavior.

Somewhat related Wang et al. [375, 376] consider two other types of nudges as well: sentiment feedback (telling users whether the message they are about to post is likely to be perceived as positive or negative) and a post timer (delaying Facebook posts by 10 seconds, which allows users to change their mind). Some of the participants in their study seemed to like these tools, but others found them intrusive and annoying.
Defaults make it more convenient for users to take the right action

Another approach to nudging users’ privacy decisions is to provide sensible defaults. Correctly chosen defaults make it easier to choose the right action, or may not even require any action at all. In this sense, defaults reduce physical [307, 349] or mental effort [364]. Defaults also provide an implicit normative cue, e.g., a default order communicates what the system thinks is most important, and a default value communicates what the system thinks you should do [240]. Finally, default values may work due to the ‘endowment effect’: people are less willing to pay for what they perceive to be a gain in privacy than what they would demand if the same decision were framed as a loss [6, 358].

Providing a certain default option nudges users in the direction of that default [349]. Therefore, while most existing work on default effects in the privacy field regards them as a nuisance, several researchers have recently suggested that they can also be used as nudges [4, 8, 23].

Empirical work on defaults as nudges is sparse:

- Knijnenburg et al. [181] showed that the odds of disclosure when social network information was shared with everyone by default were 3.9 times as high as in the private-by-default-condition, although this effect is smaller for participants with low interpersonal privacy concerns and when categories are ordered weaker ties first.
- Both Johnson et al. [157] and Lai and Hui independently showed that the sign-up rates for newsletters was about 25 percentage-points higher when sign-up was the default setting.

The order in which information requests are made can also be perceived as a default:

- Knijnenburg et al. [181] showed that the odds of disclosure when users were asked about weaker ties first were 1.8 times as high as when users were asked about stronger ties first. This “door in the face” effect confirms earlier findings by Acquisti et al. [7].
- Knijnenburg [175] found that the opposite order is more effective in sustaining disclosure when answering more questions is optional.

Nudges may threaten user autonomy

The privacy nudges evaluated in existing work show mixed results: they usually only worked for some users, and left others unaffected or even dissatisfied. Because of this, researchers argue for “smart nudges”, such as smart default settings that match the average user’s preferences [327, 332].

But what if the “average user’s privacy preferences” do not exist? In Section 1 we have cited ample evidence that people vary extensively in their information disclosure behavior, and that even for the same person this decision depends on the context in which it is made. The current
implementations of nudges, however, take a “one-size-fits-all” approach to privacy [336]: They assume that the “true cost” [155] of disclosure is roughly the same for every user, for every piece of information, in every situation. Since such nudges are rarely good for everyone, some researchers therefore argue that they may threaten consumer autonomy [327, 332].

**Recommendation:** only use nudges if there is a virtual consensus

Nudges are an interesting way to help users make the right choice without limiting their decision freedom. In most privacy settings, the “right choice” is difficult to define, though, hence nudges will not be welcomed by every user. Based on the presented analysis, we can make the following recommendations to ADL and other TLA performers:

- **Use nudges if there is a virtual consensus**—TLA-based apps should use justifications, audience feedback, and defaults on when virtually all users agree on the optimal privacy setting. In those cases, apps can use nudges to provide users choice in the unlikely event that they want a different setting after all. More intelligent forms of nudges are discussed in the next subsection.

### 6.4 User-tailored privacy

How can we reconcile the need for extensive customizability with users’ apparent lack of skills and motivation to manage their own privacy settings? This subsection discusses User-Tailored Privacy (UTP) as means to support users’ privacy decision-making (see Table 25). With UTP, a system would first measure users’ privacy-related characteristics and behaviors, use this as input to model their privacy preferences, and then adapt the system’s privacy settings to these preferences. Figure 13 shows a schematic overview of UTP.

**Table 25: Recommendations regarding user-tailored privacy**

<table>
<thead>
<tr>
<th>Employ User-Tailored Privacy to Support Users’ Privacy Decision-Making</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Determine the TLA-specific modeling factors and clusters that can be used as input for privacy modeling</td>
</tr>
<tr>
<td>- Specify adaptation strategies that will be used to implement the privacy adaptations</td>
</tr>
</tbody>
</table>
The User Privacy Model underlying UTP exploits the fact that users’ privacy behaviors are predictable. For example, several researchers have found that people’s privacy concerns are multi-dimensional, meaning that they have different preferences for different types of information [184, 199, 228, 266, 336]. In fact, research also shows that there exist distinct profiles of privacy behaviors among users [184, 266, 391]. For example, users’ public disclosure of 15 types of Facebook profile items demonstrated a 4-dimensional structure: Facebook activity (e.g. wall posts, status), Location (e.g. city, state/province), Contact info (e.g. phone number, email address), and Interests (e.g. likes, groups). Users in this dataset were clustered into 5 distinct profiles [184].

Moreover, the recipient of the information seems to play an important role in users’ disclosure decisions, both in commercial and social privacy settings [160, 181, 183, 214, 277, 377]. Again, certain “groupings” can be made. For example, for social network recipients, Knijnenburg et al. [186] found that five categories (Family members, Friends, Classmates, Colleagues, Acquaintances) resulted in the optimal solution in terms of privacy threat and usability.

Finally, in certain types of systems, privacy preferences may depend on other contextual factors. For example, researchers have found that time (weekday or weekend, daytime or evening) is an important determinant of users’ willingness to disclose their location [28, 81, 392].
Users’ behavioral patterns can be used to make privacy-related adaptations

UTP can subsequently use these patterns to provide privacy-related adaptations. These adaptations could take the form of a default setting or a recommendation, either with or without an accompanying justification:

- Knijnenburg and Kobsa [180] demonstrated the potential of “adaptive justifications”, changing the presented justification based on the users’ overall disclosure tendency and their gender. This method significantly helped users with their information disclosure decisions.
- Knijnenburg and Jin [179] used a user-tailored approach to simplify the sharing options in a location-sharing system. The study considered a hypothetical system that allowed users to “check in” to a location using one of eight sharing options. We found that reducing the number of options adaptively resulted in somewhat higher perceived decision help.
- Knijnenburg [175] studied adaptive request orders in a demographics-based health recommender system (Figure 14). The system asks demographics questions in a sequential order, and recommendations are adapted to the user’s answers on the fly. The user can skip questions if they deem them too sensitive. A study tested several means of ordering the demographics questions. Request orders that automatically trade off the usefulness and sensitivity of the items to be disclosed improved the users’ experience.

Figure 14: A demographics-based health recommender system that uses adaptive request orders to decide which demographics question to ask next
**Recommendation:** Employ user-tailored privacy when possible

The Idea of UTP fits very well within the extensive user modeling approach of the TLA. Moreover, given the complexity of the TLA, it is likely that user-tailored decision-support is the only feasible solution that allows users to maintain considerable control over their privacy decisions without overburdening them. A number of TLA-related examples may help illustrate UTP:

- The TLA normally tracks users’ location (Data) in order to give context-relevant training exercises (Organizational practice). However, UTP knows that like many young mothers (User characteristic), Mary (User) does not want her location (Data) tracked outside work hours (Other factor). It therefore turns the location tracker off by default when Mary is not on the clock (Default).
- David needs to decide how to share his recent milestones—two certificates he has recently earned (Data)—within his organization (Recipient). Due to the rules of his employer (Organizational constraint), UTP requires him to share these milestones with his direct supervisor (Recipient). Moreover, from his previous interactions (User behaviors), the UTP knows that David keeps close ties to several other divisions. UTP therefore suggests (Recommendation) that he should share his new certifications with the heads of these divisions (Recipient) as well, arguing they are likely to be interested in exploiting his newly gained skills (Justification).

UTP aims to strike the balance between giving users no control over, or information about, their privacy at all (which will be insufficient in highly sensitive situations, and may deter privacy-minded individuals) and giving them full control and information (which makes setting one’s privacy settings unmanageably complex). Arguably, UTP relieves some of the burden of the privacy decision from the user by providing the right privacy-related information and the right amount of privacy control that is useful, but not overwhelming or misleading [175]. Based on the presented analysis, we can make the following recommendations to ADL and other TLA performers:

- **Employ User-Tailored Privacy to support users’ privacy decision-making**—Employing UTP within TLA consists of two steps. First, one should determine the TLA-specific modeling factors and clusters that can be used as input for privacy modeling. This addresses the input-side of UTP. Then, one should specify adaptation strategies that will be used to implement the privacy adaptations. This determines whether the adaptations will take the form of a user-tailored justification, a smart default, or an adaptive request order.

These steps will be undertaken in version 0.2 of this document.
Conclusion

In this document, we have made recommendations regarding the Operational Characteristics of TLA-based systems that impact users’ privacy concerns. These recommendations will allow ADL and other TLA performers to select the characteristics that best alleviate users’ concerns. The recommendations in the current version of the document are tentative; the specifics of selected solutions will be added after intensive discussion with ADL and other TLA performers during the development of version 1.0 of this document.

In the meanwhile, we suggest that TLA performers pay attention to the User Characteristics of TLA users, e.g., by tailoring to different privacy management strategies and communication styles in their system designs.

Moreover, rather than collecting users’ personal information indiscriminately, TLA performers should consider Input Data Characteristics. They should make clear distinctions between the collection and use of various data types, and allow users to scrutinize and correct potential mistakes in system predictions.

TLA performers will want to present adaptations to users, and in doing this they should consider the Output Characteristics of such adaptations. For example, learning activity recommendations should be carefully planned and tailored in a way that prevents interrupting the user’s current task or leaking sensitive information.

The collection of vast amounts of information also raises question about Data Location and Ownership. TLA performers should use client-side methods for context data, and to allow users to designate a “data steward” to manage their data in accordance with their privacy preferences. TLA performers also allow users to take their data with them as they move between employers.

Moving to social and organizational aspects, TLA performers should be careful regarding Data Sharing. Specifically, they should make users aware of what information collected about them is used and how, and act ethically and responsibly regarding research placement and promotion decisions.

Finally, TLA performers should think carefully about providing Privacy Support Mechanisms, especially since the traditional paradigms of “notice and control” and “privacy nudging” seem to have failed. We propose user-tailored privacy as a way to give users more accessible yet still customizable privacy controls. Given the complexity of privacy in advanced distributed learning systems, upcoming versions of this document will delve deeper into the idea of user-tailored privacy as a decision-support mechanism for TLA.
References


90. EU 2012. Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Technical Report #2012/0010 (COD).
References


References


372. Visser, S.L. The Soldier and Autonomy. Military Medical Ethics. DIANE Publishing. 251–266.


409. Facebook real-name policy controversy. Wikipedia, the free encyclopedia.