Generic Predefined Privacy Preferences for Online Applications

Mike Bergmann

Technische Universität Dresden, Germany

Abstract. Every day users disclose various kinds of personal data using the Internet for daily activities. The disclosed data in summary may draw a perfect picture of them. Up to now it is difficult for end users to decide what to disclose and what to hide. We try to support the user in this task and propose a limited set of applicable predefined privacy preferences taking privacy principles into account. We will apply these preferences for typical online activities to evaluate and to enhance them. We elaborate the dependencies and correlations between the privacy preferences and application scenarios. As a final result and based on the proposed privacy preferences we introduce a privacy-enhancing data disclosure splitting guiding the user step by step through the process of data disclosure.

1 Introduction

Nowadays electronic communication and electronic business get more and more established. Every day users disclose personal data using the Internet for daily activities like checking timetables of public transport, doing shopping, using translation services, etc.

In the offline world, for instance, paying with cash in a shop, where the cashier does not know you, would allow you to anonymously buy goods and services. In the online world, submitting various personal data items like the item of interest, the payment and shipping information may allow to trace and to link the user's activities and may reveal user's privy preferences. Shopping becomes a privacy issue.

To enforce the right of informational self–determination in the digital world, it seems necessary to enable the user to control data disclosure and also the circumstances of the disclosure. The privacy principle of data minimization, i.e. the avoidance of the data disclosure and minimisation of the amount of data to be disclosed as a method to lower the probability of data misuse, becomes important. Privacy policies, stated by the service providers and communicated to and negotiated with the users, are introduced to express these needs and to formalize online business processes.

In the next section, we list related work relevant for our research interest. In section 3, we develop a predefined set of privacy preferences for online transactions based on today's legal and user requirements. Further on in section 4, we discuss the application of the proposed privacy preferences for typical online applications. We complement this by user interviews. We split the complex e–business process into subtasks to provide some possibilities to implement the data minimization principles. Finally the sketched wizard approach in section 5 offers a privacy–enhanced data disclosure process with further potential for user interface simplification.

2 Related work

One of the established privacy policy standards is P3P [1]. It allows expressing privacy policies in a standardized form and allows user agent based policy analysis using P3P standard terminology. A very interesting HCI approach in this context is the implementation of P3P using the bird metaphor, the so called privacy bird[2]. However, as problems we have to mention the change of privacy policies afterwards without notice and the limited negotiation capabilities. After the development of P3P, many privacy-related policy languages have been proposed [3]. Also the World Wide Web Consortium continues its work in the privacy policy area and has recently established an Interest Group on Policy Languages as part of the Privacy Activity. This group is called PLING - Policy Languages Interest Group. Its objective is the discussion and coordination of policy languages and W3Cs metadata framework. This group “will primarily focus on policy languages that are already specified and broadly address the privacy, access control, and obligation management areas; it is not expected to engage in the design of new policy or rule languages. The Interest Group will work towards identifying obstacles to a joint deployment of such languages, and suggest requirements and technological enablers that may help overcome such obstacles.” [4].

However, privacy enhancing technologies, based on complex concepts like these privacy policies, communication mixes, credentials, certificates and pseudonyms, are often not easily understood by users[5]. Additionally, a user normally has to deal with various email accounts, public/private key pairs, (cell-) phones and credit card numbers, GPS navigation devices etc. This increases the complexity, too.

In [6] were analysed the user’s protection goals. Based on these goals a set of complex user interfaces is proposed to address these goals. In [7] an approach is sketched to further simplify the process of privacy policy selection by using a town map–like approach to create a relationship between different kinds of privacy preferences and their representations in the topology of a artificial town map. There are various other approaches, like the role concept at [8] and the already mentioned P3P policies [1] etc. The PRIME project[1] is presenting a slightly different approach, combining roles and policies [9]. However, the management of dedicated privacy preferences, assigned to dedicated activities, remains difficult.

[1] The PRIME project receives research funding from the European Community’s Sixth Framework Program and the Swiss Federal Office for Education and Science. For further information see https://www.prime–project.eu/.

3 Introducing Predefined Privacy Preferences

It is a common understanding that privacy and usability can be antagonistic requirements in system design. Functional requirements are primary, usually as secondary we meet security requirement, and if generally present we meet privacy requirements behind these. Beside this, sometimes the legal privacy obligation to inform the user conflicts with the usability of the corresponding application.

For example it is not user-friendly if a system bothers the user with long explanations and never-ending terms and conditions and privacy policy documents enforcing acceptance by simply waiting until the user scrolled down the page finding the accept button at the very end of the page. However, privacy is a fundamental right of any individual in our democratic society and needs to be protected.

To assist the users to manage privacy it is important to define privacy relevant context properties on one hand and offering privacy preserving concepts, visible, perceptible and understandable by the user on the other hand. Article 6 of the EU Directive 95/46/EC [10] requires purpose binding and the necessity of data processing as significant factors to formulate a legally compliant services side privacy policy. We derive the following definitions:

Privacy policy describes the services side's official statement about the concrete data items being collected, their concrete purposes and the retention period, planned or potential data transfers possibly including further particulars. It may also contain information about the system in place to manage and protect the collected data.

As the corresponding counterpart to express client side privacy requirements we introduce the construct of privacy preferences and their instances:

Privacy preferences in summary represent the data release policy (i.e. the policy under which a user would release data) and privacy requirements a user expresses concerning possible interactions with others. They contain statements about the accepted amount of specified data items for dedicated purposes, contain conditions for transferring dedicated data items to other 3rd parties and contain statements on user-controlled linkability of different actions, i.e., for whom which user actions must, should or could be linkable or not linkable and the expected obligations and reputation[2] of the potential data receiver. The privacy preferences will be later on matched to the privacy policy of the prospective data receiver.

The privacy preferences and the privacy policy could be understood as a plug–socket system. The privacy preferences represent the plug, requiring dedicated assets, expressed by some dedicated pins (the preferences). If the privacy policy, the socket, has the corresponding holes, the plug fits. If the socket offers

[2] Obligations are e.g. the expected data retention period, secured connection, recurring audits etc. Reputation could be expressed e.g. as membership on a white list, owner of privacy seals, user experience, etc.

more additional holes (additional privacy pledges) the plug fits, too. There is no privacy conflict. But if the plug has more or other pins than the socket accepts, the system does not fit. We could see that as a privacy conflict.

Based on these definitions and with respect to the different kinds of applicable pseudonym types (transaction pseudonym, role–relationship pseudonym, role pseudonym resp. relationship pseudonym, person pseudonym [11]) now we construct privacy preferences, taking data protection law requirements, and in particular the data minimization principles, into account. We start with the most privacy friendly one and decrease the level of privacy protection in discrete steps. External definitions of what are the minimal data requirements for dedicated purposes (e.g. by data protection authorities) assist the user to follow the data minimization principles. The user selects parts of these general preferences and applies it to the concrete application case before starting the disclosure as the basis for the privacy policy negotiation. To make it even more comfortable we assemble a collection of four predefined privacy preferences:

(α) **No PII:** Personal Identifying Information (PII) are not released, transaction pseudonyms are used, i.e. user actions are linkable by the service provider only within a dedicated transaction. The user may decide afterwards to connect transaction pseudonyms to become linkable. Reading a weblog or editing a Wikipedia entry anonymously [12] (see also the blog scenario description in section 4) are examples where such privacy preference could be applied[3].

(β) **No PII, but linkable:** PII are not released. Transactions are linkable by the service provider using the provided (role–) relationship pseudonyms as defined in [11]. However the communication itself works pseudonymously. Data about personal preferences (and pseudonyms) might be released (which are not directly identifying the user). Prominent examples are web mailers, various news panels (see the email application scenario in section 4) etc. The more data becomes linkable, the more difficult it becomes for the user to remain not identifiable.

(γ) **Disclose only necessary PII:** Only PII to fulfil the purpose of primary service are released. No "sensitive" data should be disclosed[4]. Beyond that, a strict "no further transfer" policy should be applied to other recipients to avoid data leaking. To take the today's distributed service architectures[5] into account we extend it to "trusted[6]" communication partners with the user's explicit consent only. The communication becomes linkable. A well

[3] We assume the standard TCP/IP connection is anonymized, e.g. using JAP [13] and no other user identification (via cookies etc.) is possible.

[4] Sensitive in the meaning according to the definition of Art. 8 [10] and additionally according to the perception of the user. The personal data should contain a corresponding sensitivity flag that a user could apply.

[5] Distributed service architecture with dedicated partners for order fulfilment, goods delivery and payment processing.

[6] What "trusted" means for a user, has to be specify in the privacy preferences. It could be some personal reputation, the presence of privacy seals, trusted hardware

known example where these privacy preferences could be applied is to buy a book online (see the e–shopping application scenario in section 4).

(δ) **Disclose additional PII:** Personal data may be released also for additional services[7]. Data are released only to "trusted" communication partners according to the user's trust policy. Transfer to other recipients should be controlled (e.g. only with the user's explicit consent) or only transfer to "trusted" recipients. "Sensitive" data are excluded. An example is a participation in a customer care program to get bonus points or other benefits.

Table 1 shows the concrete privacy preferences. The first column is numbering the preferences. The second column contains a short description about the data that should be released, the third column states whether the user acts anonymously, pseudonymously or identifiably, the fourth column contains the data release policy applied to the data.

	PII	Relationship	Purpose and Transfer
α	no PII	anonymous	not applicable
β	no PII, but user name, password, further additional non–identifying personal data	pseudonymous	only for current purpose[8] and no transfer
γ	sufficient (but not sensitive) PII	pseudonymously or real identity	only for current purpose and strict no further transfer
δ	additional (but not sensitive) PII	pseudonymously or real identity	for additional purposes and strict no further transfer

Table 1. The predefined privacy preferences

In α and β, PII are not disclosed at all. However, personal data that are indirectly released, such as a collection of search strings, a click stream, some special personal preferences like favourite colour, interests etc. may lead to a significantly reduced anonymity set and therefore to an re–identification of the subject [14].

etc. A more simple approach could just trust all partners fulfilling the same or stricter privacy policies.

[7] Additional means the data are not necessary to fulfil the primary service intent, i.e. data are requested to offer additional services, like for marketing or advertisement, for suggesting related topics, collecting bonus points etc. This does not mean a full or uncontrolled data disclosure

[8] "Current purpose" is defined [1] as the usage for completion and support of activity for which data was provided; Information may be used by the service provider to complete the activity for which it was provided, whether a one-time activity such as returning the results from a Web search, forwarding an e–mail message, or placing an order; or a recurring activity such as providing a subscription service, or allowing access to an online address book or electronic wallet.

In the next section, we will instantiate the discussed privacy preferences in context to concrete applications to apply the proposed concrete privacy preferences and compare them to the services side privacy policies.

4 Applying the Predefined Privacy Preferences

Applying the four pre–defined privacy preferences we have to define suitable online applications. An internal PRIME privacy preferences survey [15] was performed to elaborate the current situation and to help finding these suitable online applications[9]. The survey confirmed the expectation that users percept Internet business scenarios as more privacy invasive as e.g. mobile phone applications or native desktop applications. The survey furthermore elaborated, which are the most popular online services in general and which are the usually required data items to disclose[10] for such services in particular.

According to the results of the study we selected the online applications, listed below, for our further elaboration. We have to mention that these examples are not covering the whole variety of online applications and not ordered yet. They do not exclude each other and may be combined. The user should be able to define the missing preferences based on our predefined privacy preferences.

e–shopping: Applicable for buying physical and digital goods. The amount of PII to disclose depends on the services, usually *reliable PII*[11] are required for shipping and billing purpose. e–shopping in general is used *pseudonymously, but identifiable*. The applied privacy policy limits PII usage to the stated *current purpose* with possible *transfer to associated 3^{rd} parties*, applying the same privacy policy as for the service, to fulfil the business processes. Normal e–shopping accounts like accounts at Amazon or Apple iTunes are examples for this.

Social network: Applicable for social networks about music, photo, video sharing etc. There are *no PII* necessary, but is expected to increase the trustworthiness from the perspective of other peers. In general a *pseudonymous, non-identifying* account is used. The applied privacy policy is less strict compared to e–shopping. The data often are intentionally used for *additional purposes* too, like statistical, marketing etc. The data could be *transferred to associated 3^{rd} parties.* Prominent examples are Skype, YouTube, MySpace, SecondLife etc.

Download: To download software (but also MP3 files, videos, pictures etc.) if payment is not mandatory. *No PII* are required, but often requested.

[9] 35 persons from various countries of the European Union took part in the survey. We are aware of the fact that this small number of participants in general, and the PRIME project members in particular are not representative for this kind of survey, but it holds as a starting point for further research.

[10] We analyse the concrete PII request only. Further content, released by the data subject, like the text itself in a blog for instance, is not taken into account.

[11] We could require certified PII, but this is less usual in the explored scenarios.

The data are therefore not sensitive and could be fictive (false name, e–mail, phone number etc.) Ideally an *anonymous* account is used. The privacy policy may have some additional marketing aspect included, consequently the purpose is extended to *marketing purpose* with possible *transfer to 3rd parties.*

Blog: Read, edit and create new comments in a news forum or blog. There is *no PII* identifying the user. The usage is performed under *pseudonym or even anonymously.* The applied privacy policy often states *further purposes* beside the current purpose and *allows transfer* to 3$^{\text{rd}}$ parties.

e–mail: Used to access so called free–mail or e–mail accounts to write e–mails, to configure the spam filter and to fill the address book. There are *no PII* required, but during usage the collectable data could become identifying, especially address data, contact information, personal interests and other[12]. The applied privacy policy allows *additional purposes and transfer* to associated 3$^{\text{rd}}$ parties. The released data could be *sensitive*[13]. Prominent examples are Yahoo or Google mail services for instance. Especially the "Google Mail" privacy policy [16] does not comply with our understanding of a user– and privacy–friendly data handling policy[14].

Membership: To get access to restricted resources like special web pages etc. *PII* is required. The access is provided *pseudonymously*, but based on the PII the user could be identified. The service privacy policy limits the PII usage to the *current purpose* with *no transfer* to 3$^{\text{rd}}$ parties. Examples are automotive and sports club membership etc.

Further: Application scenarios like *infrastructure, licensing, collaboration, news* are of less frequent usage and fit into one of the above mentioned scenarios. We do not list them here separately.

Application	*PII usage and account requirements*	*Purpose*	*Transfer*	coverd by
Download	no PII, anonymous	additional	to other parties	α
Blog	no PII, pseudonymous	additional	to other parties	β
e–mail	no PII, pseudonymous	additional	to trusted 3$^{\text{rd}}$ parties	β
Membership	PII, identifying	current	not allowed	γ
e–shopping	PII, identifying	current	to trusted 3$^{\text{rd}}$ parties	γ
Social network	PII, identifying	additional	to trusted 3$^{\text{rd}}$ parties	δ

Table 2. The application's typical privacy policies and the applied privacy preferences

[12] We assume that all content is encrypted so the content itself could not be read.

[13] Could be for instance information about health status, about membership in an alcoholism self–helping group etc.

[14] Besides this, the Google privacy policy bases on different legal grounds (US law instead of European law). But as the Google services are really widely distributed used and accepted we took such non–European application scenarios also into account.

Table 2 groups the selected example applications mentioned above. It shows the association of the predefined privacy preferences from section 3 with the privacy policies of the online applications. It shows that the predefined privacy preferences cover the sketched applications. However we made the following implicit assumptions about some of the parameters:

- Transfer of PII to 3rd parties, not applying the same privacy policy as the service (lets call it *suspicious party*), is excluded. This means, in case of an involvement of an strange party (e.g. by the presence on a black list or by simply being unknown to the user), the user has to decide about the relationship to the 3rd party. Doing so the user could either accept the new party (and thereby transfer the situation towards a valid predefined preferences application) or reject the service.
- As transfer to "any party" is not provided for, if PII is affected, we have to state that some services are not covered at all by the proposed privacy preferences. If the user releases PII to such services, like the Google e–mail service for instance, the privacy preferences settings do not fit [16].
- There is no pre–configuration for sensitive PII. In case sensitive PII is affected, the user has to decide it separately and manually to take the sensitivity into appropriate consideration. So we intentionally excluded it from the predefined privacy preferences. The same holds for other special service conditions and configurations.

In this section we elaborated the introduced predefined privacy preferences and associated them to privacy policies of typical online applications. We discussed the necessity of PII, the usual purpose binding and data transfer policy for each example. In the following section we will show, how the predefined privacy preferences (γ) can be applied in practice. Further on we discuss a further potential privacy enhancement by splitting data disclosure requests into their basic data disclosure elements. A concrete example implementation is given.

5 Predefined Privacy Preferences Implementation

A conventional e–shopping application contains various subtasks. Subtasks for instance are *Order, Payment* and *Shipping*. If there are further 3rd parties involved, more subtasks may be defined (address verification, certification, subcontracting etc.). To perform the shopping process, quite a lot of data are necessary. Applying the discussed "strict no further transfer" policy, as discussed in section 3, privacy preferences γ, service scenarios become impossible because of the need to transfer PII to 3rd parties to fulfil the service. To solve this contradiction we split the data disclosure into subtasks.

5.1 Privacy enhancing data disclosure splitting

Usually there is no need for the shop vendor to know the customer's address or payment information. If we split the business process into the three mentioned separate parts *Order, Payment* and *Shipping*, like shown in Table 3, every involved party gets the data needed. The separation of processes on the need-to-know basis for enhancing the users privacy has been proposed also in academic concepts (e.g., Chaum 1985 [17]; Pfitzmann/Waidner/Pfitzmann 1990/2000 [18]; Clauß/Köhntopp 2001 [19]) as well as in practical specifications such as the Secure Electronic Transaction standard (SET 1997 [20]) or as a use case in the Liberty Alliance project (Foll 2007 [21]), which is developing specifications for federated identities and identity-based Web services.

In Figure 1 we sketched a possible communication flow in case we split the data disclosure process as described. The subtasks are interconnected by each other by so called transaction IDs. Using different IDs for different subtasks we avoid an unintended linkability between the involved parties. The benefit of the split for the user is obvious. The data are only disclosed to the party related to the business and limited to the purpose for which the data was released and could be tailored for the very special business purpose. Also from the service provider's point of view it becomes much easier to be legally compliant – if less data are collected less data have to be protected etc. In our example very few personal details at all should be disclosed to the shop. Table 4 explains the details. In summary, splitting the business process into subtasks offers the benefit that only the minimal amount of data is released to all involved parties. Instead of sending all data to the shop (which then would have to transfer data to payment and shipping providers), the shop gets only to know the list of ordered items from the

Ordering a book at www.bookstore.net:

Data	Communication Partner	Policy
Pseudonym (e.g. customer number), item of interest e.g. ISBN	Merchant/Service provider, for example www.bookstore.net	Only for "current" purpose, in our case selling a book; no further transfer, secure data storage not longer as legally required

Payment with credit card

Data	Communication Partner	Policy
Credit card number, expiry date, real name, amount of money	Payment service provider, for instance www.cash.eu	Only for "current" purpose, in this case payment; no further transfer, secure data storage not longer as legally required

Delivery of the good to a specified address

Data	Communication Partner	Policy
Address of the client and the (covered, hidden) good, i.e. the item of interest is not known	Shipping service provider, for instance www.ups.com	Only for "current" purpose, in our example to deliver the good; no further transfer, secure data storage not longer as legally required

Table 3. Business process splitting into subtasks

Step	Description	Communication Details
1	The user makes the initial request to place an order. He sends an identifier of the resource to be ordered. In our case he requests a book using the ISBN Number.	the ISBN Number to address the resource.
2	The service provider informs the user about the access conditions for the resource. As far as the final cost may depend on other facts (like shipping in this example), first he informs about all possible shipping partners.	Transaction IDs ('A' and 'B') as the identifying handles; Description of the next step and further on a list of accepted third parties like DHL, UPS, FedEx etc.
3	The user contacts the shipping provider of his choice and requests a transport commitment token (credential).	Transaction ID 'A' to enable partners to link the process and the address details of the sender and recipient.
4	In this simplified version the shipping provider contacts the service provider directly using the address details to get additional parameters (like weight and size) to calculate the costs.	The shipping provider sends a parameter request using the Transaction ID 'A' for authentication and a list of required parameters.
5	The service provider sends the desired parameters back.	Transaction ID 'A' for linkability and list of concrete parameter details.
6	As we use a simplified version the shipping provider sends the token directly to the service provider. In a more privacy enhanced version the shipping provider may send the token to the user and the user forwards it to the service provider. A more general example may get the payment directly from the user; it just copies the payment steps, see below. The benefit is that the request (see step 2) could contain all necessary information (cost, size, weight etc.) and does not need further communication for parameter updates.	Transaction ID 'A' for authentication, the shipping credential (like an "e–Stamp" to certify and to prove the successful shipping arrangement) and the concrete costs for shipping.
7	Repeats step 2 with details about the payment procedure. The service provider provides additional payment parameters (the concrete costs) directly. Applying this to step 2 could make step 4 and 5 obsolete.	Transaction ID 'B' for assigning the payment to the transaction; Payment information and accepted payment partners.
8	The user contacts his payment provider to send a dedicated amount of money to the service provider.	Transaction ID 'B' for authentication; Details like Sender, Receiver of the payment and amount of money to pay.
9	The payment provider issues the corresponding credential (like a cheque) and send it to the service provider.	Transaction ID 'B' for authentication; Payment credential.
10	After the service provider received all necessary access tokens, in our case payment and shipping credentials, the physical good is shipped to/picked up by the shipping provider.	Transaction ID 'A' for linkability; the final delivery.

Step	Description	Communication Details
11	An order confirmation is sent to the user.	Transaction ID ’A’ and ’B’ for linkability.
12	The shipping company delivers the good. The payment provider should deliver the payment. This is not shown in this example.	Transaction ID ’A’ for authentication and the delivery itself. The order process is finished.

Table 4. Communication Details for Figure 1

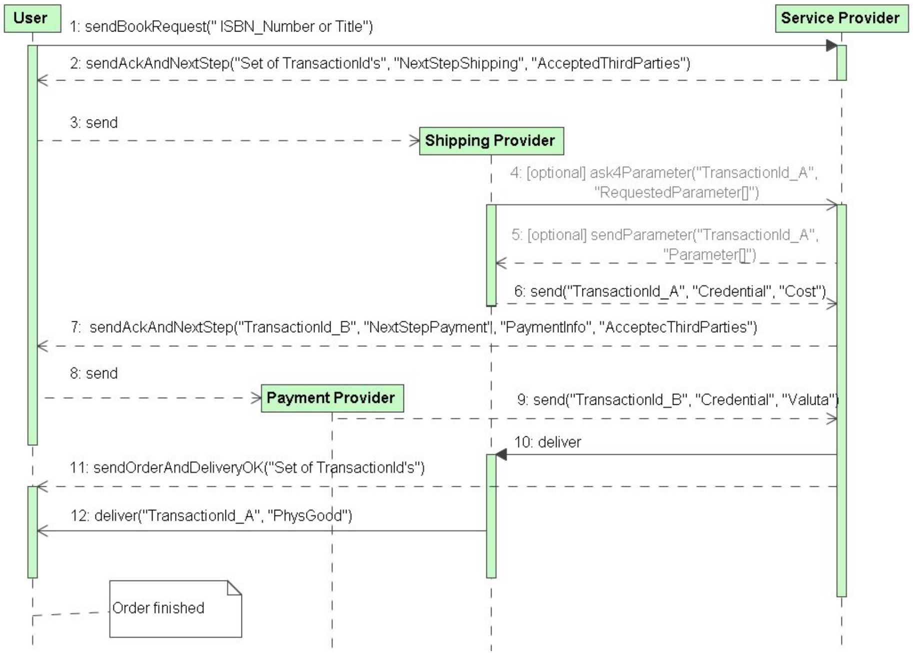
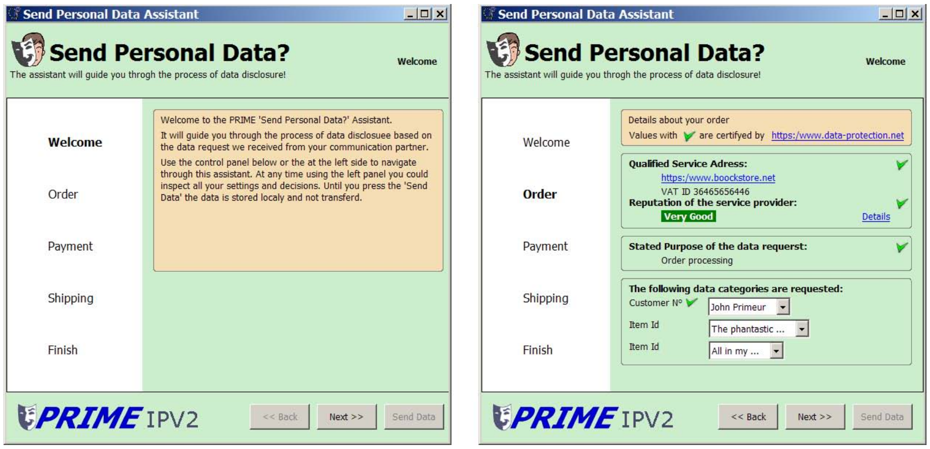

User
Service Provider
1: sendBookRequest(" ISBN_Number or Title")
2: sendAckAndNextStep("Set of TransactionId's", "NextStepShipping", "AcceptedThirdParties")
3: send
Shipping Provider
4: [optional] ask4Parameter("TransactionId_A", "RequestedParameter[]")
5: [optional] sendParameter("TransactionId_A", "Parameter[]")
6: send("TransactionId_A", "Credential", "Cost")
7: sendAckAndNextStep("TransactionId_B", "NextStepPayment", "PaymentInfo", "AcceptecThirdParties")
8: send
Payment Provider
9: send("TransactionId_B", "Credential", "Valuta")
10: deliver
11: sendOrderAndDeliveryOK("Set of TransactionId's")
12: deliver("TransactionId_A", "PhysGood")
Order finished

Fig. 1. A possible sequence diagram for our split scenario

user, while the shipping providers received the address data and the payment provider receives the payment details directly from the user. This implements the strict no-transfer policy that we have foreseen for the predefined privacy preference (see γ). It helps to increase the privacy in general and to fulfil the privacy principle of data minimization in particular.

5.2 The “Wizard–like” Approach

In the introduction we promised to structure identity management processes towards enhancing privacy and to simplify the user interactions regarding privacy and identity management at the same time. However in the previous section, we have split the action “buying a book” into tree different actions with different service providers (see Figure 1). At first glance it seems to contradict to the idea of simplification. We solve this issue by introducing a wizard–like approach assisting and guiding the user through the decision making process. The assistant presents a sequence of decision requests according to the privacy preferences of the end user to compile a finally instantiated privacy policy. A short pilot user test confirmed that users percept the splitting into subtasks as simplifying the process and increasing the transparency. Further user tests should examine this statement in more detail.



The assistant will guide you throgh the process of data disclosure!

Welcome to the PRIME 'Send Personal Data?' Assistant.

It will guide you through the process of data disclosuee based on the data request we received from your communication partner.

Use the control panel below or the at the left side to navigate through this assistant. At any time using the left panel you could inspect all your settings and decisions. Until you press the 'Send Data' the data is stored localy and not transferd.

The assistant will guide you throgh the process of data disclosure!

Details about your order

Values with ✓ are certifyed by https:/www.data-protection.net

Qualified Service Adress: ✓
https:/www.boockstore.net
VAT ID 36465656446

Reputation of the service provider: ✓
Very Good

Stated Purpose of the data requerst: ✓
Order processing

The following data categories are requested:

Customer N° ✓	John Primeur
Item Id	The phantastic ...
Item Id	All in my ...

Fig. 2. An example “Send Personal Data” Assistant

As shown in Figure 2 the assistant informs the user about the overall procedure. It collects all the required PII, shows the dedicated purpose of the data request and allows to walk through the different stages to check the settings, made before. It possibly shows also available information about the service provider (e.g. seals or reputation data), about the requested certificates as well as the data handling policies and obligations. In our example the dialogue contains sections with the statements about data recipient, stated purposes and required personal data. The wizard in Figure 2 receives the dedicated data request provided by the service provider. Using the predefined privacy preferences here, offers the advantage that users do not have to define their preferences themselves from the scratch, but jut have to chose one of the predefined ones. It instantiates our privacy preferences (γ) for an e-shopping application could then warn the users if for instance more data is requested than needed for the specific service. Thanks to the predefined preferences it becomes easy to gather and maintain the user's privacy requirements even for users not primarily interested in privacy.

6 Conclusion

In this paper we provide a set of predefined privacy preferences, helpful for deriving applicable instances of dedicated privacy preferences for various online applications. The user could simply choose from these instead of defining privacy preference by hand repeatingly. By using the predefined preference the system could then warn the users if the service provider does not behave as predefined in the preferences.

Besides this, we proposed an approach for structuring privacy–related data disclosure processes in a more privacy–friendly way then before. The developed wizard-based UI approach is guiding the user through this process. The special focus to the strict "no transfer, only for the stated purpose" policy enhances the privacy of the user.

Further user acceptance tests will help to improve and fine–tune this approach. Additional tests to check whether the wizard approach really simplifies the data disclosure and privacy policy understanding will supplement the work.

7 Acknowledgment

Thanks to our colleagues for the helpful comments. Special thanks to the team of the Technische Universität Dresden, namely Andreas Pfitzmann, Sebastian Clauß and Thomas Kriegelstein, to Simone Fischer-Hübner and John Sören Pettersson from the Karlstad University, Sweden, to Lothar Fritsch from Johann–Wolfgang–Goethe–University Frankfurt/Main, to Marit Hansen and Jan Schalaböck from Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, the PRIME–internal survey participants and all others contributors for the very helpful discussion.

References

1. W3C. Platform for Privacy Preferences, April 2002. Online available at http://www.w3.org/TR/P3P/.
2. L. Cranor. P3P: Making privacy policies more useful. *IEEE Security and Privacy*, pages 50–55, 2003.

3. Marit Hansen and Ammar Alkassar. A study on network protocols and privacy-aware communication. Technical report, FIDIS Deliverable D3.8, Frankfurt/Main, November 2007.
4. W3C Policy Language Interest Group. PLING Charter. available online at http://www.w3.org/Policy/2007/ig-charter.html.
5. A. Whitten and J.D. Tygar. Why Jonny Cant Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the Ninth USENIX Security Symposium*, 1999.
6. Gritta Wolf and Andreas Pfitzmann. Properties of protection goals and their integration into a user interface. In *Computer Networks: The International Journal of Computer and Telecommunications Networking*, volume Volume 32, pages 685–700, New York, NY, USA, May 2000. Computer Networks, Elsevier North-Holland, Inc.
7. Mike Bergmann, Martin Rost, and John Sören Pettersson. Exploring the feasibility of a spatial user interface paradigm for privacy-enhancing technology. In *Proceedings of the Fourteenth International Conference on Information Systems Development*, Karlstad, August 2005. Springer-Verlag.
8. Sebastian Clauß and Thomas Kriegelstein. Datenschutzfreunliches Identitätsmanagement. *DuD Datenschutz und Datensicherheit*, 27:297, 2003.
9. John Sören Pettersson, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauß, Thomas Kriegelstein, and Henry Krasemann. Making PRIME usable. In *Symposium on Usable Privacy and Security*, Carnegie Mellon University, Pittsburgh, PA, USA, July 2005. Carnegie Mellon University.
10. Council of Europe. Data Protection Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Online available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
11. Andreas Pfitzmann and Marit Hansen. Anonymity, unobservability, and pseudonymity - a proposal for terminology. In *Proceedings of WS on Design Issues in Anonymity and Unobservability*, Designing Privacy Enhancing Technologies, LNCS 2009, Proceedings of the Fourteenth International Conference on Information Systems Development, Heidelberg, August 2001. LNCS. Revised version 0.29 of July, 31st 2007; Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology; available at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.
12. Wikipedia. Help:Contents/Getting started – Wikipedia, The Free Encyclopedia, 2007. [Online accessed 19-May-2007] http://en.wikipedia.org/wiki/Help:Contents/Getting_started.
13. O. Berthold, H. Federrath, and M. Köhntopp. Project “Anonymity and Unobservability in the Internet”. In *Proc. Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000*, pages 57–65, Toronto/Canada, April 4-7 2000. ACM.
14. Michael Barbaro and Tom Zeller Jr. A face is exposed for AOL searcher No. 4417749. *New York Times Online*, August 2006. http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=11754 00000&en=fd9b0c3b15c36970&ei=5070.
15. Mike Bergmann. PRIME internal privacy preferences survey about privacy concerns and conditions. In *Technical Report TUD-FI07-04-Mai 2007*, Technische Universität Dresden, Saxony, Germany, May 2007. Technische Universität Dresden. http://dud.inf.tu-dresden.de/˜mb41/publications/TUD-FI07-04_Mai2007.pdf.

16. Google Inc. Google Mail Privacy Policy, 2007. Online; accessed 20-May-2007; http://mail.google.com/mail/help/intl/en-GB/privacy.html.
17. David Chaum. Security without identification: Transaction systems to make big brother obsolete. In *Communications of the ACM*, volume 28, No. 10, pages 1030–1044, October 1985.
18. Birgit Pfitzmann, Michael Waidner, and Andreas Pfitzmann. Rechtssicherheit trotz Anonymitt in offenen digitalen Systemen. *Datenschutz und Datensicherung DuD*, 14/5-6:243–253, 305–315, 1990. translated into English: Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity, IBM Research Report RZ 3232 93278) 05/22/00, IBM Research Division, Zurich (May 2000).
19. Sebastian Clauß and Marit Köhntopp. Identity management and its support of multilateral security. *Computer Networks*, 37:205–219, 2001.
20. SET Secure Electronic Transaction LLC. The set standard specification, May 1997. originally at http://www.setco.org/set_specifications.html; now mirrored at http://www.cl.cam.ac.uk/research/security/resources/SET/.
21. Fulup Ar Foll. Liberty Alliance From Usecases to Specifications, Jan 2007.