Toward Applying Online Privacy Patterns Based on the Design Problem: A Systematic Review

Maha Aljohani[1(✉)], James Blustein[1,2], and Kirstie Hawkey[1]

[1] Faculty of Computer Science, Dalhousie University, Halifax, Canada
mh578194@dal.ca, {jamie,hawkey}@cs.dal.ca
[2] School of Information Management, Dalhousie University, Halifax, Canada

Abstract. Privacy patterns are design solutions to common privacy problems—a way to translate "privacy-by-design" into practical advice for software engineering. This paper aims to provide a collection of privacy patterns proposed by previous work through a systematic review. The review identifies 19 research papers on privacy patterns and they were retrieved for full-text analysis based on the type of the privacy pattern, the context, design problem, and the proposed solution. We provide a classification of the privacy patterns by applying a mapping process to the ISO 29100 privacy Framework and the Privacy Enhancing Techniques. We found that the currently available patterns barely reference to privacy legislation or laws. They mostly cover the security-network perspective but not the user interface perspective. This paper presents the results of a systematic, comprehensive review that aims at aiding future IT designers with a collection of privacy patterns to match design contexts and benefit from the proposed privacy design solutions.

Keywords: Privacy patterns · Privacy-by-design
Privacy Enhancing Technologies (PETs)

1 Introduction

Privacy is an emerging design element for interactive systems [1]. Researchers have been studying privacy from different aspects such as privacy-preserving technologies [2–4], e-commerce [5], Healthcare [6, 7]. There are variety of privacy design guidelines to support the integration of privacy in the design lifecycle such as Privacy Impact Assessment (PIA) [8], ISO 29100 Privacy Framework Principles [ISO] [9], Process-Oriented Strategies and Privacy Enhancing Tools (PET) [10]. However, there is a lack of the "end-to-end" solutions to design privacy-preserving systems and the challenge is "in turning these broad guidelines into actionable design solutions" [1].

We are interested in investigating the currently available privacy patterns as privacy design solutions. This paper aims to provide a collection of privacy patterns proposed by previous work through a systematic review. In addition, we discuss how the Privacy Patterns are connected to Privacy Principles and Privacy Enhancing Technologies.

A. Marcus and W. Wang (Eds.): DUXU 2018, LNCS 10918, pp. 608–627, 2018.
https://doi.org/10.1007/978-3-319-91797-9_43

2 Background

In this systematic review, we are analyzing the currently available privacy patterns. As a preliminary to the review, we introduce the Privacy Principles, and Privacy Enhancing Technologies (PETs) to be able to make a comprehensive comparison between these three concepts. Privacy Principles and guidelines are used to describe how organizations handle privacy while Privacy Enhancing Technologies are focused on privacy from a technical point of view. Privacy patterns are in between.

2.1 Privacy Principles

Privacy principles are privacy framework that can be discussed to understand what is privacy and what are the privacy requirements [11]. There are variety of privacy principles around the world such as OECD Privacy Principles which is common in European Union, Asia-Pacific Economic Cooperation (APEC) Privacy Framework which is used in the Asia-Pacific region, the United States Department of Commerce Safe Harbor Privacy Principles, and Generally Accepted Privacy Principles (GAPP) which is popular among Canadian privacy practitioners. They all share basic principles including collection limitation, data quality, purpose specification, use limitation, safeguards, openness, individual participation and accountability principles. ISO 29100 is an example of privacy principles that share the same privacy principles with the previously mentioned privacy frameworks and discussed in the following Table 1.

Table 1. ISO 29100 privacy framework

#	Principle	Definition
1	Consent and choice	Present data subject with choices to obtain consent
2	Purpose legitimacy and specification	Insure following legislations and inform data subjects of the purposes to process the Personal Information
3	Collection limitation	Limit the collection of data to the specified purposes
4	Data minimization	Minimize the amount of data collected and the number of actors involved in processing the data
5	Use, retention and disclosure limitation	Limit the use, retention and disclosure of personal information
6	Accuracy and quality	Ensure data is accurate, up to date, and relevant Periodically check the data
7	Openness, transparency and notice	Provide access to information, inform of the policies in place and provide notices whenever there is a change
8	Individual participation and access	To provide opportunity to access and review personal information
9	Accountability	Inform if there is a privacy breach, apply privacy policy, and provide training
10	Information security	Provide a level of security by applying protocols
11	Privacy compliance	The system meets the legal requirements and applies supervision mechanisms

2.2 Privacy Enhancing Technologies (PETs)

Borking and Raab [12] defined PET as a "system of ICT [Information and Communication Technology] measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system." The European Commission adopted the same definition in 2007. The purpose of developing new privacy enhancing technologies is to protect the privacy of users and at the same time allowing them to still share and communicate through the Internet. Some examples of these technologies are summarized next.

Anonymizer is a type of PETs that remove all personal information to preserve users' privacy; it helps users to browse the Internet without their identity being disclosed. Such systems use one of the following mechanisms to ensure anonymity: anonymous proxies, anonymous/pseudonymous servers and firewalls [13]. One such system is available at <URL: https://www.anonymizer.com/>. The idea of using proxies is to create an account with a "trusted" Internet Service Provider in which both the user and the organization trust. One type is location anonymizer, which works in a way that it hides users' information and replaces pseudo-identifier [14]. For example, if the user wants to go visit Google, he/she does not send a request to the Google server. Instead, the request is made through the anonymizer server, which connects to Google server and forwards the information to the user. It has many advantages including not sending a user's IP address, not forwarding the user's email as an identifier, and eliminating all cookies that might be stored in the user device. Another PET example that uses the same concept is iProxy, which is available at iProxy.net.iProxyanonymizer service http://iproxy.net/.

Crowds is a system that helps users to browse the Internet while protecting their privacy by grouping users into diverse crowds to hide personal information. This prevents attackers from tracking the source of information and requests [14]. The anonymizer relies on using a proxy that it is installed in a local machine or online; the primary objective of Crowds is to browse anonymously by hiding the information about both the user and the information shared from servers and third parties [15]. The idea of crowds relies on hiding individual actions with actions of other individuals [15]. For example, if user A sends a message to a server, Crowds sends the message as it is from a random member which prevents the server from detecting the real sender [15].

Platform for Privacy Preferences (P3P). P3P was initially proposed and developed by The World Wide Web Consortium [16]. The platform is designed in a way that helps users understand how their personal information is used by websites. It compares a website privacy policy and a user's privacy policy to help the user to decide whether to share their information or not. However, it does not alert the user, nor set minimum standards for privacy. The tool should be tested to measure the success of using P3P in solving privacy problems [16]. There are a variety of tools that were developed and implemented based on P3P summarized from [13] including:

- Netscape 7.0 which disclose the privacy policy of the website and inform the user about the cookies used.

- JRC P3P Version 2.0, which controls access to servers according to privacy preferences that are initially set up by the user.
- AT&T Privacy Bird helps users to be informed about how their personal information is collected and used.

There are a variety of PETs that serve the same goal of protecting users' privacy over the Internet which include GUIDES (EU Data Protection Directive (95/46/EC)—DPD.), Privacy Incorporated Software Agent PISA (http://www.tno.nl/instit/fel/pisa.), and GAP [17]. There are variety of examples of PETs such as 'onion routing' [18].

2.3 Definitions of Actors

We adopted the classification of the European Directive on Data Protection (2007) and the Italian privacy authority portal (2005) that defined different actors who would be involved in data processing including:

- Data Subject (DS): an individual or a person who has the rights to share, manage and control personal information
- Data Controller (DC): the person who decides in which and how data are processed
- Data Processor (DP): a person or an individual who process data on behalf of the data controller.

These definitions were used to identify different roles in the process of proposed solutions to the privacy patterns.

3 Research Objectives

Privacy designers face challenges in applying privacy-preserving techniques. The main goal of the study is to support the concept of Privacy-By-Design (PbD) [19] by providing privacy designers and developers with currently available privacy preserving patterns to apply in early design lifecycle. A supporting goal is to validate whether the proposed Privacy Patterns can be mapped to worldwide standards-based methodologies (e.g., ISO 29100) [9] to answer the questions: What privacy principles are guaranteed if the system design followed the privacy patterns from the literature? We want to compare the privacy patterns and Privacy Enhancing Techniques (PETs) to identify how they are intertwined and what aspects of privacy patterns are covered by the PETs.

4 Method and Analysis

A systematic review was conducted using ACM, IEEE, Science Direct, and Springer libraries to identify proposed privacy patterns that propose solutions for privacy design problems. A total of 200 references were screened. The papers that were candidate for inclusion in the systematics review were read more comprehensively to decide to include them. After applying exclusion criteria, 19 were retrieved for full-text analysis.

We adopted the format of the POSA2 on all collected patterns because it includes all elements that designers and developers need when they search for solutions to solve

design problems. Following one structure will help designers and developers to adopt and use these patterns when they share the same context, problem, solution, and will help to understand the consequences and challenges they would face. The patterns are formatted using the order: context, problem, solution, known uses, and consequences. We added the related or similar patterns section because we believe that patterns should not contradict, and they are connected to each other to provide solutions to the same problem, and by draw connections between patterns in the literature, we provide richness and increase comprehension level to designers in case they want to apply the patterns to their contexts. We list the patterns that share the same or part of the solution which provides useful classification in our literature review according to the solution.

5 Results and Discussion

We have listed 19 privacy patterns. They are included because they are the most popular and have well-known uses. Privacy patterns are: Informed Consent for Web-Based [20], Masked Online Traffic [20], Obtaining Explicit Consent Pattern [21], Access Control to Sensitive Data Based on Purpose [21], Minimal Information Asymmetry [20], Privacy Dashboards [22], Instant User Interface for Information about Personal Identification Information [23], Non-repudiation Pattern [25], Data abstraction [23], Ambient notice and Private link [22], Outsourcing [24], Notification, and limit disclosure [26]. Privacy patterns are "design solutions to common privacy problems—a way to translate "privacy-by-design" into practical advice for software engineering". In typical design lifecycle, privacy patterns are implemented in the design and implementation and recommended to be applied in the early during requirement analysis and architectural design [27]. Some of the patterns can be linked to the privacy from the legal perspective as discussed in Sects. (5.12, 5.13, and 5.14). However, the literature lacks in this domain and a few number of patterns were found to cover the legal perspective. The results of the systematic review include the following privacy patterns and the relationship between them is shown in Fig. 1.

5.1 Informed Consent for Web-Based Transaction Pattern

The pattern is proposed by Romanosky et al. [20]:

Context. A web designer or developer wants to create a website that collects personal information for surveys and registration. The Data Controller wants to protect the DSs' personal information because laws and it is under the US regulation.

Problem. When collecting personal information, websites usually use cookies. DSs are concerned that their personal information would be collected and used without their consent or do not want to share their personal information. The problem relies on how the designers would communicate their goals of using the information without ignoring the DSs' concerns.

Solution. To solve the problem, the web designer should provide the DS with the following elements:

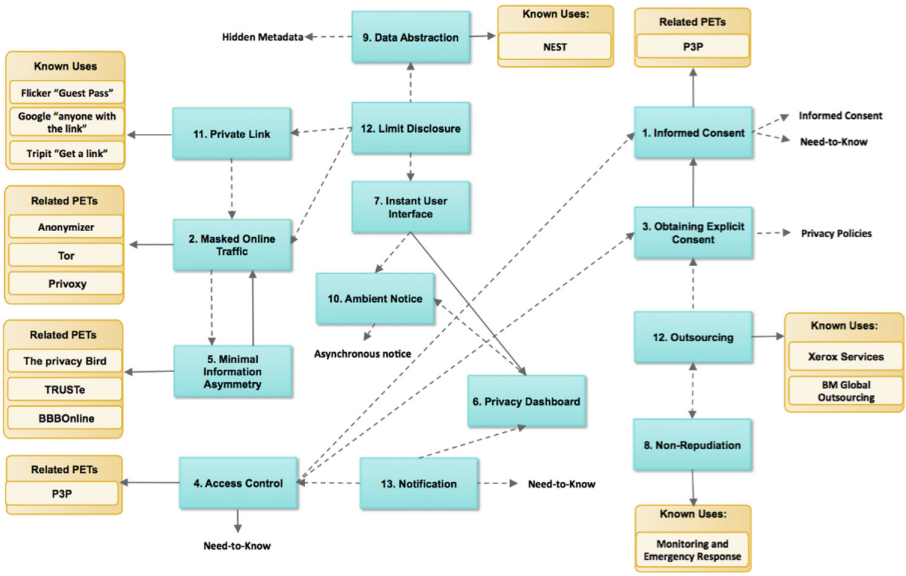

Fig. 1. The relationship between the privacy patterns, their known uses and related PETs

Disclosure. To help DSs know how the information will be collected: explicitly by asking DSs to provide the information or implicitly by their IP address or cookies.

Agreement. To be able to opt-out at any time without being concerned that the information will be used without permission or maintained for a longer time.

Comprehension. To ensure that DSs know how this information would be collected, what are cookies, and for what purpose the information is collected.

Voluntariness. To not manipulate the DS by not offering a certain service unless they provide their personal information and provide the DS with other alternative options in case they have some questions about being asked to provide the information (e.g., online chat-center or telephone number to contact a representative).

Competence. The DS is eligible (e.g., age restrictions) to provide the information that is being collected.

Minimal Distraction. To not distract the DS from completing the main task.

Known Uses. The pattern has been used in many well-known websites, (i.e., Yahoo, Google, and ehealthinsurance.com) during the filling of the registration form. The form explains to the DS why specific information needs to be filled. For example, Yahoo has an informative box near to the birthday selection to explain to the DS why the website needs to have the DS's birthdate, which will be used in the future for account verification as shown in Fig. 1.

This pattern matches the Fair Information Practices (FIP) deployed by many website privacy policies and laws (Federal Trade Commission Report 2000). It is

consistent with using P3P as an automated platform to match between the website privacy policies practices and DS preferences. Another use is by developers or technical support of desktop applications that require DSs' information for further assistance about installation or other activities (Fig. 2).

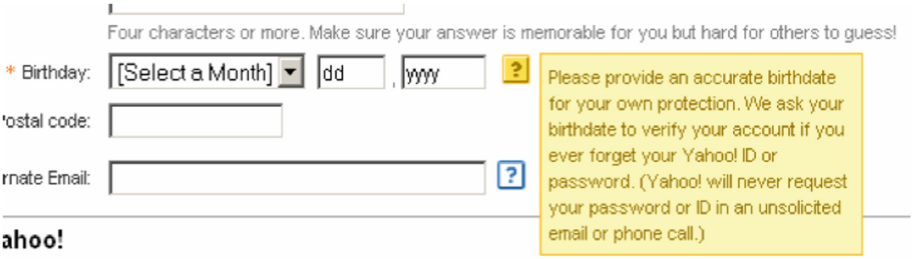

Fig. 2. Yahoo registration adopted form (yahoo.com)

Consequences. The pattern has two benefits: it helps in reducing the amount of information collected from the user (Data Subject) by the organization (Data Controller), and it helps in building trust between them by providing explanations about why their information is being collected. The pattern suffers from limitations that include: it does not help DSs to stop the use of the information at any time (opting-out). Some websites do not want to explain why they collect the information to allow them to use it. The website budgets might not cover all the expenses to cover every element in the pattern.

Related/Similar Patterns

- Informed Consent (Fischer-Hübnner et al. 2010) and [24]. Both patterns are related in one aspect because they focus on providing the Data Subject with a consent stating purposes of collecting the PI.
- Need-to-Know pattern [24] focus on limiting the access to the PI by Data Processors (third parties) for only specified permission.

Therefore, the Informed Consent for Web-Based Transaction Pattern covers more than stating the purposes and access by permission. It covers opting in and out from an agreement by understanding how the information is collected with minimal distraction from the main task.

5.2 Masked Online Traffic

The pattern is proposed by Romanosky et al. [20]:

Context. The Data Subject want to browse the Internet but does not want to reveal more personal information than necessary. The DS is concerned about the information privacy. DSs are aware of some applications and technologies that would protect their privacy but are not sure when and how to use them.

Problem. How the Data Subject can minimize the amount of personal information sent over a public network. The following forces should be considered:

- The message sent by DS might not be revealed, but information associated with it would reveal information about the DS.
- The DSs do not have to be a network or technology expert to hide their information over the network.
- The DS wants to have a solution that is easy to use.

Solution. To use one of following techniques:

Anonymity Techniques. To help the DS to communicate but still be unidentified. Two types of systems can be used: anonymizing systems, which help DSs to be completely anonymized to parties; and pseudonymous systems, which help DSs to not be identified as individuals.

Blocked Requests. Software tools can block cookies and web bugs that are used to track users.

Known Uses. One popular PET applications that ensure anonymity include:

- Anonymizer (www.anonymizer.com). The application offers a launching connection to other websites on behalf of the DSs without revealing of any personal information.
- Tor (https://www.torproject.org) applies Onion Routing protocol, which uses many routers to encrypt the requests and process it in many layers.
- Privoxy (www.privoxy.com). It acts as a virtual server that prevents cookies, and banners ads.

Consequences. The pattern includes many benefits: the applications offered as solutions are not complicated, and do not require technical knowledge. They require only a basic knowledge of how to install and configure a desktop application. Another benefit is that DSs can interact with online websites and still be anonymized. The pattern suffers from limitations that include: using anonymizing proxies to interact on behalf of the DS means that these proxies collect and monitor the DS's communication through the network. Using Tor offers extra layers and routers over the network to process the request, which might decrease the interaction performance. Some websites require identification information (i.e., online banking) in which a use anonymizing protocols would not be suitable.

Related Patterns. Minimal Information Asymmetry [20] is related to the aspect of providing the DS with enough information about a service or a tool that will collect the information to help the DS make decisions to allow or deny the collection (Sect. 5.5).

5.3 Obtaining Explicit Consent Pattern

The pattern is proposed by Porekar et al. [21]:

Context. DSs want to use an industrial medical application that collects sensitive data about patients and which is regulated by the organization privacy policy.

Problem. How can the organization collect the information without disclosing patients' information without gaining DSs' permission?

Solution. Agreement between the Data Subject (user) and Data Controller (organization) needs to be accomplished by implementing three elements:

Agreed Privacy Policy. After forming the privacy policy, the DS can negotiate the content either automatically or in person.

Signatures of Both Parties. Once the DS agrees on the privacy policy, both sign the agreement.

Timestamp. Once it is signed, a time stamp is created in case the organization wants to change/edit some parts, DSs are informed and the process starts again.

Known Uses. No known uses.

Consequences. The application employs a *Certificate-of-Liability* that explains the converge and limitation of the consent, which allows DSs to sue the organization in case of misuse of the sensitive information.

Related Patterns that Deal with Privacy Policies [21]

- Constructing Privacy Policy-building the terms and conditions of the privacy policy
- Maintaining Privacy Policy-explaining the reasons for these conditions and terms and maintaining agreements over longer periods of time
- Privacy Policy Negotiation-negotiation between the two actors who use and apply the policy.

Similar Patterns. Informed consent [24] patterns are related in the aspect of the need of providing consent to collect the information. The pattern differs in adding details to the consent (i.e., signature and timestamp).

5.4 Access Control to Sensitive Data Based on Purpose

The pattern is proposed by Porekar et al. [21]:

Context. The organization is collecting the sensitive data according to a specific purpose that should be clear to the DS.

Problem. How can the organization make the purpose clear to the DS and allow the DS to have a level of control over what is collected? The DS determines the amount of personal data that will be collected. The DS can decide which part of information a third party can access and hide the other part of the information.

Solution. The pattern applies the *"Need-to-know"* technique to limit the amount of sensitive information transmitted to third parties. The pattern provides access to only the data for which the DS gives permission to be shared and the third party does not

have the right to access the information that the DS wants to hide. This pattern depends on an agreement between DS and organization about what to make available to third parties and what to hide.

Known Uses. Platform for Privacy Preferences (P3P) [16].

Consequences. The pattern supports the benefit of giving the DS a level of control over what they want to share over the internet by third parties according to an agreed privacy policy. However, how the DS would know if the organization allowed a third party to collect the information and use them? What would guarantee that they do not do so?

Related Patterns that Deal with the Agreement Are

- Obtaining Explicit Consent [20] is related in one aspect, which is providing consent, but it takes the solution further to cover extra aspects (i.e., signature and timestamp).
- Informed consent [24].

Similar Patterns. Need-to-know pattern [24] is the same pattern that provides the same solution.

5.5 Minimal Information Asymmetry

The pattern is proposed by Romanosky et al. [20]:

Context. The Data Subject is in some online services to buy products or services, and wants to register to be able to access the services. These services include subscriptions to local news, events, online banking, and health insurance. The Data Subject is interested in having feedback on the process of the information collection and the agreement statement on the Data Controller's websites. The Data Subject is discouraged to start using the website due to the lack of information.

Problem. The problems associated with this context are as follows: the DS wants to perform a purchasing task and wants to have a feedback about the privacy policy before inserting any personal information. Second, the DS is concerned about future privacy violations after the purchase is completed, and the transaction should be safe and accomplished easily. Third, the DS does not want to provide more sensitive information than necessary while following the purchase steps.

Solution. The DS can acquire more information about the websites that apply both *Informed Consent* and *Signals*.

Informed Consent. Websites that apply the "Informed Consent for Web-Based Transaction" can provide the DS with all the information they need and provide the ability to opt-in and out from the website services.

Signals. Signals are messages that are provided by the business to inform the DS about either the product or the agreement. The DS must recognize these signals and use them to gather the information. Examples of such signals include money-back guarantees, warnings, and privacy policies.

Known Uses.

- The privacy Bird (search.privacybird.com)
- TRUSTe (www.truste.org)
- BBBOnline (www.bbbonline.org).

Consequences. Benefits of this pattern include reducing the risk of privacy violations by helping the Data Subject to make the right decisions after getting proper feedback about privacy policy of the websites and services.

Related/Similar Patterns. Masked Online Traffic- to reduce the amount of information transmitted to others [20]. It is discussed in detail in Sect. 5.2. This pattern is used as the first part of the solution along with the signals for the Minimal Information Asymmetry.

5.6 Privacy Dashboards

The pattern is proposed by Privacypattern.org [22]:

Context. There is an organization that collects personal information about DSs and these information changes over time. The methods used by the organization to collect the information are unexpected or invisible. The pattern allows DSs to access and browse the information.

Problem. DSs are asked to enter personal information without an explanation provided to them on how these data will be collected and used. DSs are not confident or sometimes are overwhelmed. DSs need to understand what is going behind the scene regarding data collection.

Solution. An informational privacy dashboard to provide DSs with information about what is collected and how their information is processed. It can be used to provide a visual representation of the personal information and how it is handled. This gives DSs the ability to view, correct, and delete their personal information. Privacy Dashboards answer the DS's question "what do you know about me?".

Known Uses. Google Privacy Dashboards (https://www.google.com/dashboard) as shown in Fig. 3.

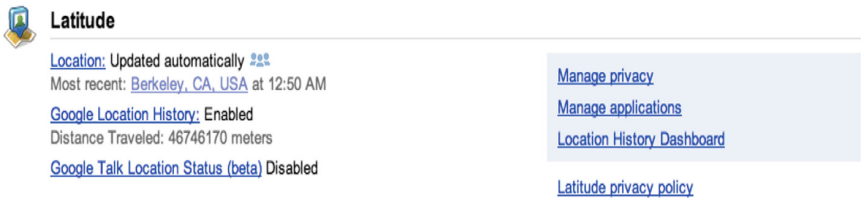

Fig. 3. Google privacy dashboard (https://www.google.com/dashboard)

Consequences. Using this pattern might create new privacy issues such as providing personal information to others (i.e., other users, third parties, stalkers). Designers should balance between showing information to the user and ensuring that the personal information refers only to that user.

Related/Similar Patterns. Ambient notice [22] is discussed in Sect. 5.10.

5.7 Instant User Interface for Information About Personal Identification Information

The pattern is proposed by Bier and Krempel [23]:

Context. The personal information is collected and processed by the online technology service. The data Subject should understand enough of the system design to be informed about how the system collects and processes the personal information.

Problem. The system collects and processes the personal data through complex transactions. It is difficult for a typical user to understand when and why the data is collected. The system stores personal information in sensors and these sensors (servers) might not be in one place.

Solution. Informing the Data Subject about the sensor that collects and processes the data during the communication. It would help the DSs to understand that the information is placed in a sensor, and they can access the information anytime for any reason.

Known Uses. Privacy Dashboard such as Google Privacy Dashboards (https://www.google.com/dashboard) but the Instant User Interface pattern focuses on informing the DSs about the location where their information is stored.

Related/Similar Patterns. Ambient Notice [22] is related to the concept of providing a DS with a feedback, which is discussed in Sect. 5.10.

5.8 Non-repudiation Pattern

The pattern is proposed by Compagna et al. [25]:

Context. When the Data Controller performs its own tasks by dividing the tasks into subtasks and relays the responsibilities of DSs information protection/processing to parties or actors according to predefined relations. The DC (organization) needs a commitment from the Data Processor (third party/agent) to preserve DS's privacy but the Data Controller does not have any guarantee that the supplier takes the responsibility to achieve and provide commitment.

Problem. The Data Controller must have evidence that the Data Processor cannot repudiate the pre-defined commitments.

Solution. The solution is to gain this commitment through two parts:

- Part 1: is a proof of commitment when the data controller delegates the responsibility to the data supplier.

- Part 2: is a trust that is initiated between the two actors and any failure of fulfillment can be returned to the proof presented by the supplier in the first part.

Known Uses. Monitoring and Emergency Response Centre (MERC) in any healthcare system.

Related/Similar Patterns. The Outsourcing Pattern [24] is related to the pattern in the aspect of the agreement to process information with DP as discussed in Sect. 5.12.

5.9 Data Abstraction

The pattern is proposed by Bier and Krempel [23]:

Context. The data processing occurs in different levels of abstraction and data storage varies in different forms.

Problem. The second use of data (personal information) is a great threat of DSs' privacy. Who is allowed to access the data when it is stored?

Solution. To perform data abstraction, which helps in reducing the amount of information stored and collected. Data abstract can help in revealing only what is needed for specific tasks.

Known Uses. NEST video abstraction & fusion [30].

Related/Similar Patterns. Hidden Metadata [31] is related in the aspect of network encryption method by hiding the personal information transmitted over the network.

5.10 Ambient Notice

The pattern is proposed by [22]:

Context. When the DC performs ongoing tracking of DS's locations or can access DSs' location at any time.

Problem. When the DS's location information is used as a repeated model dialog with or without the DSs' permission. How can DSs get a notice about every time a service is using location information?

Solution. The solution is an ambient notice that appears instantly when location information is retrieved. The notice should provide an opportunity to interact with the permissions.

Known Uses. Location-based services icons used in Mac OS.X. It is shown as a compass arrow that appears in the taskbar every time an application is used to track the DS's location as shown in Fig. 4.

Fig. 4. Ambient location services icon in Mac OS X [22] (privacypattern.org, 2014)

Consequences. Providing the DS with overwhelming details is a disadvantage of this pattern and notices might be annoying.

Related/Similar Patterns. Asynchronous notice [22] which shares the same context and solution.

5.11 Private Link

The pattern is proposed by [22] Privacypattern.org (2014):

Context. When the DS wants to share content to a group of users (public, or part of the public), and the private content can be accessed regularly.

Problem. The DS wants to limit the number of people who can access the private content available online.

Solution. The DS is provided with a private link or un-guessable Uniform Resource Locator (URL). Only a pre-authorized DS who has the link can access the personal information. The DS decides on who can access the information.

Known Uses

- Flicker "Guest Pass" (https://help.yahoo.com/kb/SLN13039.html)
- Google "anyone with the link" sharing (https://support.google.com/drive/answer/2494893?hl=en)
- Tripit "Get a link" (https://www.tripit.com).

Consequences. Security requirements should be implemented to ensure that only the authorized group can access the content.

Related/Similar Patterns. The Masked Online Traffic [20] is discussed in Sect. 5.2.

5.12 Outsourcing

The pattern is proposed by Compagna et al. [24]:

Context. The Data Controller (organization or a website owner) outsources the data processing practices to a Data Processor (third party).

Problem. Only the DC is responsible to perform the data processing. How can the organization transfer the rights to the Data Processor (DP) without provoking DS's privacy?

Solution. The outsourcing can be legal if the DP agrees to a data processing contract, which must be signed by both the DC and the DP (third party). This means that the DC has to inform the DS about which data will be shared or processed with other parties.

Known Uses

- Xerox Services "IT Outsourcing" (http://services.xerox.com/it-outsourcing/enus.html)
- BM Global Outsourcing Services (http://www-935.ibm.com/services/us/en/it-services/outsourcing.html).

Consequences. The DSs need to be informed and their consents need to be gained before applying the pattern. In some cases, the DS's consent is not gained and the DP still can access without permission. Another issue might arise which is what is the case would be if the DP rejected to agree on the data processing agreement. The solution is to associate this pattern with the Non-Repudiation Pattern [25].

Related Patterns

- Obtaining Explicit Consent [20] and Informed consent [24] are related to this pattern in the need to provide a consent whenever sensitive data is processed.
- Non-repudiation Pattern [25] is related in one aspect by defining the tasks and subtasks that should be accomplished by DP according to an agreement to process DS personal information.

5.13 Limit Disclosure Privacy Pattern

The pattern is proposed by Aljohani et al. [26].

Context. The DS has the right to get access to a list of activities carried out on their information (have a list of who accessed the information) and can to request to not disclose information (choose from the list).

The pattern is applied in healthcare applications and personal health information. The DS agrees on sharing the information with some health agents and organizations and to limit the access to a well-identified list of agents.

Problem. The DS wants to balance between what is shared and who can gain access. The secondary use of information shared between organizations without consent concerns the DSs.

Solution. By being able to limit the organizations that can access the information the privacy pattern protects DS's health information. It allows for limiting the information shared over organizations as follows:

Access Control. The DS requests a record of activities that have been done on the PHI regarding the list of agents who accessed the information. The DC retrieves the information either from a third party, which should be gained from an earlier agreement or from the organization server. The DS has the ability to: agree on the list, or; limit the list by choosing from the list (blocking some), and request not to disclose at all to any of them. Individuals would be able to choose the information that they decide they would like to reveal and mask the rest by providing levels of disclosure.

Authentication. The system applies two-steps identity clarification technique to lock out unauthorized access and/or modification as a security measures.

Consent. The DSs have to sign a consent on the responsibilities associated with not disclosing information because it is associated with personal health information. The DC has to confirm changes and provide feedback.

Feedback. The feedback feature should be applied to inform and notify DSs of the ongoing changes in case there is a new setting.

Related Patterns

- The Masked online traffic pattern by [20] allows users to control what information to reveal and minimize the amount of personal information shared (Sect. 5.2).
- Data abstraction pattern by [23] allows individuals to control whom to reveal the information and provide feedback on who has access to the information (Sect. 5.9).
- Private link pattern by [22] works in limiting who can see the personal health information (Sect. 5.11).
- Instant user Interface by [23] allows individuals to opt in or opt out (Sect. 5.7).

5.14 Notification Privacy Pattern

The pattern is proposed by Aljohani et al. [26].

Context. The individual under this right is being notified of unauthorized activities performed on his/her personal health information.

Problem. The collected information should be used for the purpose that it was collected for and should not be accessed/and or processed for other purposes. The DS wants to be informed instantly in case of secondary use of information, which includes stolen information, lost or subjected to unauthorized access, use, disclosure, copying, or modification.

Solution. To design a privacy-preserving application, two aspects should be investigated: the system-server aspect and user-system aspect. In case of the system-server, the system should apply the Secure Socket Layer (SSL) to protect it from unauthorized access. In case of the user-system, to prevent unauthorized modification the system should apply two-step identification process.

Notification and Consent. The DS is notified in different situations classified according to the type of the practice, which includes; information is stolen or lost as one type, information use, disclosure, copy, and modified as another type. The last type is being subjective to unauthorized access.

Consequences. The DS is informed about the list of activities and agents who are performing these activities and the DS has to agree on collecting the information before the collection with an indication of clear purposes. A challenge of the pattern is that it does not prevent the unauthorized access before it occurs. It focuses on providing feedback when it occurs to help the DS make decisions on next steps to recover the breach. Some security measures should be already installed by the organizational.

Related Patterns

- Need-to-know informs users about recent activities done on the personal health information [24].
- Access control by [21] informs users about the requests to access the information (Sect. 5.4).
- Privacy dashboard and ambient notice by [22] allows users to be informed on how and why the information is collected (Sect. 5.6).

5.15 Mapping Privacy Patterns to ISO Privacy Framework

It is important to identify the difference between Privacy Enhancing Technologies (PETs) and privacy patterns. PETs solve only one specific privacy problem in already implemented software while privacy patterns are design frameworks and guidelines that can be used in similar contexts [28]. Because the there is a lack of methods to validate privacy patterns, we evaluate the proposed privacy patterns according to ISO29100 privacy framework and Privacy Enhancing Techniques. Privacy patterns that are based on a legal framework and focuses on the design of UI are rare.

Only two papers were based on privacy from a legal perspective [24, 26]. Therefore, there is a need to translate privacy from a legal perspective into privacy in the IT perspective. The literature review lacks in this domain. The current state of severe problems around the world in managing personal information has created a gap between the privacy regulation requirements and Information Technology designers [29]. To bridge the gap, designers need to evolve data protection practices throughout the system design process, which relates to the concept of Privacy by Design (PbD) [19] and privacy patterns (Table 2).

Table 2. Mapping privacy patterns to ISO privacy framework

Patterns	ISO 29100 privacy principles								
	Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability
1.	✓	✓	✓	×	✓	×	✓	✓	✓
2.		✓	✓	✓	×	✓		✓	✓
3.	✓	✓	✓	×	×	✓	✓		✓
4.		✓	×	×	✓	×	✓	✓	×
5.	✓	✓	×	×	✓	×	✓	✓	×
6.	×	✓	×	×	×	×	✓	✓	×
7.	×	×	×	×	✓	✓	✓	×	✓
8.	×	✓	✓	×	✓	✓		×	×
9.	×	×	✓	×	✓	✓	✓	✓	×
10.	×	✓	×	×		×	✓	×	×
11.	×	✓	✓	×	✓	×	✓	×	✓
12.	✓	✓	✓	×	✓	×	✓	✓	×
13.	✓	✓	✓	×	✓	×	✓	✓	×
14.	✓	✓	✓	✓	×	×	✓	✓	✓

5.16 Privacy Patterns Categorization

The privacy patterns are classified according to two concepts: the stakeholder for which the problem was described (a user, organization developer, and/ or system designer); and into which privacy principle they belong. The classification adds to the literature by shedding the lights on the patterns that propose solutions to solve the privacy design problem from the user's perspective, not the security-network perspective. In the following table, we summarize the categorization of the privacy patterns in Table 3.

Table 3. Privacy patterns classification

Privacy pattern	Problem according to	Privacy principle
Informed consent for web-based transaction pattern	Designer	Access, transparency, and feedback
Masked online traffic	End users	Encryption
Obtaining explicit consent pattern	Organization developer	Notice
Access control to sensitive data based on purpose	Organization developer	Access
Minimal information asymmetry	End users	Minimization and user control
Outsourcing	Organization developer	
Privacy dashboards	End users	Access, transparency, and feedback
Instant user interface for information about personal identification information	End users	User interface and transparency
Non-repudiation Pattern	Organization developer	Access
Data abstraction	Designer and organization developer	Minimization
Ambient notice	End users and organization developer	Transparency and user control
Private link	End users	User control

6 Conclusion

We presented a systematic review of the currently available privacy patterns mapped to IDO privacy principles and PETs. The currently available patterns focus on proposing implementation solutions for privacy problems in specific contexts. They barely reference to the legal legislation or laws on which they are based. They focus on how to

implement privacy through a security-network perspective and they do not address privacy from the end user's perspective. We believe conducting the systematic review of currently available privacy patterns will provide Information Technology (IT) and UI designers and developers with a privacy framework to help them to apply according to their matching design contexts.

Acknowledgments. This work has been funded by the University of Jeddah in Saudi Arabia, with the support of the Saudi Cultural Bureau in Canada.

References

1. Iachello, G., Hong, J.: End-user privacy in human–computer interaction. Found. Trends® Hum.-Comput. Interact. **1**(1), 1–137 (2007)
2. Yang, J.J., Li, J.Q., Niu, Y.: A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener. Comput. Syst. **43**, 74–86 (2015)
3. Liu, X.Y., Wang, B., Yang, X.C.: Survey on privacy preserving techniques for publishing social network data. J. Softw. **25**(3), 576–590 (2014)
4. Bao, L., Zhang, D.Y., Wu, J.B.: Internet of things and privacy preserving technologies. Electron. Sci. Technol. **23**(7), 110–112 (2010)
5. Aïmeur, E., Brassard, G., Fernandez, J.M., Onana, F.S.M.: A lambic: a privacy-preserving recommender system for electronic commerce. Int. J. Inf. Secur. **7**(5), 307–334 (2008)
6. Lu, R., Lin, X., Shen, X.: SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Trans. Parallel Distrib. Syst. **24**(3), 614–624 (2013)
7. Anderson, C., Agarwal, R.: The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Inf. Syst. Res. **22**(3), 469–490 (2011)
8. Clarke, R.: Privacy impact assessment: its origins and development. Comput. Law Secur. Rev. **25**(2), 123–135 (2009)
9. ISO/IEC 29100: Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27
10. Hoepman, J.-H.: Privacy design strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds.) SEC 2014. IAICT, vol. 428, pp. 446–459. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55415-5_38
11. OECD: Excerpts from Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data are © OECD 1980 (1980)
12. Borking, J.J., Raab, C.D.: Laws, PETs and other technologies for privacy protection. J. Inf. Law Technol. **1**, 1–14 (2001)
13. Seničar, V., Jerman-Blažič, B., Klobučar, T.: Privacy-enhancing technologies—approaches and development. Comput. Stand. Interfaces **25**(2), 147–158 (2003)
14. Damiani, M.L.: Privacy enhancing techniques for the protection of mobility patterns in LBS: research issues and trends. In: Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.) European Data Protection: Coming of Age, pp. 223–239. Springer, Dordrecht (2013). https://doi.org/10.1007/978-94-007-5170-5_10
15. Reiter, M.K., Rubin, A.D.: Crowds: anonymity for web transactions. ACM Trans. Inf. Syst. Secur. (TISSEC) **1**(1), 66–92 (1998)
16. W3C: Platform for Privacy Preferences, P3P 1.0 (2002). http://www.w3.org/P3P/

17. Bennett, K., Grothoff, C.: GAP – practical anonymous networking. In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, pp. 141–160. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40956-4_10
18. Communication COM: 228 from the Commission to the European Parliament and the Council. On Promoting Data Protection by Privacy Enhancing Technologies (PETs) (2007)
19. Cavoukian, A.: Privacy by design: leadership, methods, and results. In: Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.) European Data Protection: Coming of Age, pp. 175–202. Springer, Dordrecht (2013). https://doi.org/10.1007/978-94-007-5170-5_8
20. Romanosky, S., Acquisti, A., Hong, J., Cranor, L.F., Friedman, B.: Privacy patterns for online interactions. In: Proceedings of the 2006 Conference on Pattern Languages of Programs, p. 12. ACM, October 2006
21. Porekar, J., Jerman-Blazic, A., Klobucar, T.: Towards organizational privacy patterns. In: 2008 Second International Conference on the Digital Society, pp. 15–19. IEEE, February 2008
22. Privacypattern.org
23. Bier, C., Krempel, E.: Common privacy patterns in video surveillance and smart energy. In: 2012 7th International Conference on Computing and Convergence Technology (ICCCT), pp. 610–615. IEEE, December 2012
24. Compagna, L., El Khoury, P., Krausová, A., Massacci, F., Zannone, N.: How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. Artif. Intell. Law **17**(1), 1–30 (2009)
25. Compagna, L., Khoury, P.E., Massacci, F., Thomas, R., Zannone, N.: How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach. In: Proceedings of the 11th International Conference on Artificial Intelligence and Law, pp. 149–153. ACM, June 2007
26. Aljohani, M., Hawkey, K., Blustein, J.: Proposed privacy patterns for privacy preserving healthcare systems in accord with nova scotia's personal health information act. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 91–102. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39381-0_9
27. Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S.: Tales from the dark side: privacy dark strategies and privacy dark patterns. Proc. Priv. Enhanc. Technol. **2016**(4), 237–254 (2016)
28. Chung, E.S., Hong, J.I., Lin, J., Prabaker, M.K., Landay, J.A., Liu, A.L.: Development and evaluation of emerging design patterns for ubiquitous computing. In: Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, pp. 233–242. ACM, August 2004
29. Aljohani, M., Blustein, J., Hawkey, K.: Participatory design research to understand the legal and technological perspectives in designing health information technology. In: Proceedings of the 35th ACM International Conference on the Design of Communication, p. 39. ACM, August 2017
30. Moßgraber, J., Reinert, F., Vagts, H.: An architecture for a task-oriented surveillance system: a service-and event-based approach. In: 2010 Fifth International Conference on Systems (ICONS), pp. 146–151. IEEE, April 2010
31. Hafiz, M.: A collection of privacy design patterns. In: Proceedings of the 2006 Conference on Pattern Languages of Programs, p. 7. ACM, October 2006