PRIAM: A Privacy Risk Analysis Methodology

Sourya Joyee De, Daniel Le Métayer

▶ **To cite this version:**

Sourya Joyee De, Daniel Le Métayer. PRIAM: A Privacy Risk Analysis Methodology. [Research Report] RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes. 2016. hal-01302541

HAL Id: hal-01302541
https://inria.hal.science/hal-01302541

Submitted on 14 Apr 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

PRIAM: A Privacy Risk Analysis Methodology

Sourya Joyee De and Daniel Le Métayer

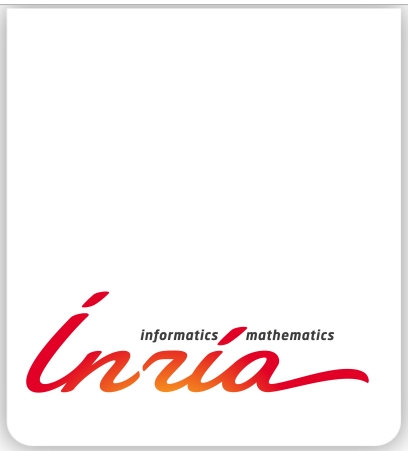
RESEARCH REPORT

N° 8876

Avril 2016

Project-Team PRIVATICS

ISSN 0249-6399 ISRN INRIA/RR--8876--FR+ENG



PRIAM: A Privacy Risk Analysis Methodology

Sourya Joyee De and Daniel Le Métayer

Project-Team PRIVATICS

Research Report n° 8876 — version 1.0 — initial version Avril 2016 — revised version Avril 2016 — 47 pages

Abstract: Privacy Impact Assessments are recognized as a key step to enhance privacy protection in new IT products and services. They will be required for certain types of products in Europe when the future General Data Protection Regulation becomes effective. From a technical perspective, the core of a PIA is a privacy risk analysis (PRA), which has so far received relatively less attention than organizational and legal aspects of PIAs. In this document, we propose a framework and methodology for conducting a PRA which is both rigorous and systematic and illustrate it with a quantified self use-case.

Key-words: privacy, personal data, privacy impact assessment, PIA, risk, harm, regulation, law, quantified self

RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

PRIAM: Un cadre d'analyse de risques d'atteintes à la vie privée

Résumé : La nécessité de conduire une analyse d'impact (PIA) avant tout déploiement de système ou de service informatique présentant des risques potentiels d'atteinte à la vie privée est désormais reconnue. Les analyses d'impact sur les données personnelles deviendront d'ailleurs obligatoires pour certaines catégories de produits quand le nouveau règlement européen sur la protection des données personnelles entrera en vigueur. L'analyse des risques en matière de vie privée, qui doit constituer la partie technique d'un PIA, a jusqu'à présent été moins étudiée que les aspects juridiques et organisationnels des PIAs. Ce rapport de recherche décrit une proposition de cadre et de méthodologie pour conduire ces analyses de risques d'atteinte à la vie privée de manière rigoureuse et systématique. Ce cadre, appelé PRIAM (Privacy Risk Analysis Methodology) est illustré avec un cas d'étude dans le domaine du "quantified self".

Mots-clés : vie privée, données personnelles, analyse d'impact, risque, préjudice, loi, droit, quantified self, mesure de soi

Contents

1 Introduction

Most of the new IT products and services deployed nowadays rely on the use of personal data. If appropriate measures are not taken, they can therefore lead to a variety of privacy breaches [29, 30, 40]. To ensure that such risks are properly understood and addressed, there is a growing recognition that a privacy impact assessment (PIA) should be conducted before the design of a product collecting or processing personal data. According to Clarke [3], a privacy impact assessment is *"a process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and examined"*. Several countries like Canada, the USA and the UK [51] have played leading roles in this movement. Europe has also promoted PIAs in areas such as RFIDs [6] and

smart grids [8] and is strongly emphasizing privacy and data protection risk analysis in its up-coming General Data Protection Regulation (GDPR) [1] [39]. Beyond legal requirements, conducting a PIA is a recommended step for any company intending to deploy a potentially sensitive system or service. By contrast, several examples have shown in the past that too hasty deployments trigger strong public opposition [1, 10, 13].

There is already a large body of contributions on PIAs and a number of PIAs for specific products have been published [6, 8]. For example, D. Wright proposes a sixteen-step optimized PIA process based on a review of various existing PIA methodologies [50]. Official bodies such as the CNIL and NIST have also published PIA guidelines [11, 19, 20, 21]. All these contributions are very useful to establish the general framework and to help the experts in the organization of a PIA process (including planning, stakeholders consultation, resource allocation, audits, etc.) and its main goal (evaluating the likelihood and severity of privacy threats). However, they do not define very precisely how the technical part of the PIA (Privacy Risk Analysis, or PRA, here) should be perfomed.

The objective of this paper is precisely to fill this gap and propose a framework and methodology for conducting a PRA which is both rigorous and systematic. In addition, great care has been taken to keep this framework, that we call PRIAM[2] , concrete, customizable and compatible with most existing PIA recommendations.

The framework relies on the definition of appropriate *categories* and *attributes* of seven components (*system*, *stakeholders*, *data*, *risk sources*, *feared events*, *harms* and *privacy weaknesses*). The methodology is made of two main phases: *information gathering* and *risk assessment* leading to a well-defined risk assessment process based on *harm trees*.

In Section 2, we provide an overview of our PRA methodology. In Section 3 and Section 4, we describe it and illustrate it on our running example. We discuss related works in Section 5 and conclude in Section 6.

2 Overview of PRIAM

Since security is an essential component of privacy, there are a number of commonalities between a privacy risk analysis and a security risk analysis. However, privacy is a more complex, multifaceted concept aiming at the protection of people (individuals, groups and society as a whole) and regulated by laws. These dimensions must be taken into account in a privacy risk analysis, especially the notion of privacy harm which has been extensively discussed by lawyers but not really integrated within existing PRAs.

We believe that the two main challenges to conduct a PRA are (1) the consideration of all factors that can have an impact on privacy risks and (2) the appropriate assessment of these impacts and their contribution to the assessment of the overall risks. To address these challenges, the PRIAM framework revolves around a collection of seven components, each of them being associated with (1) a set of *categories* from which the relevant elements have to be chosen for a given system and (2) a set of *attributes* which

[1] Conducting a PIA will become mandatory for certain categories of personal data processing.
[2] PRIAM stands for Privacy RIsk Analysis Methodology.

have to be defined and used for the computation of the risks. The seven components are the following: the *system*[3], the *stakeholders*, the *data*, the *risk sources*, the *privacy weaknesses*, the *feared events* and the *harms* (see Figure 1). The system and the set of stakeholders are the inputs of the analysis.

The *categories* of a component are useful to find all the relevant elements (types of components) for a given system. For example, data categories include, among others, health data, location data, financial data and contact data; stakeholder categories include data subjects, data controllers, data processors and third parties. The *attributes* of a component refer to the aspects of the component that can have an effect on privacy risks. For example, the *precision* level and the *retention* delay of the personal data collected by a system can affect the likelihood of a risk of privacy breach. Figure 1 shows for each component[4] the associated attributes[5]. Table 10 (Appendix A) summarizes the categories and attributes of all the components in PRIAM.

In addition to their direct contribution to the evaluation of privacy risks, attributes can be used to determine the relevant categories for other components through *attribute-category* links (see Figure 1) or to determine the attributes of other components through *attribute-attribute* links[6]. Some attributes play a primary role, whereas others only play a weak or supportive role in determining the category or attribute of another component. These roles are pictured by *strong* and *weak* links respectively in Figure 1. For example, the *functional specification* of a system completely defines the categories of data being processed by the system (solid line). In contrast, the *origin* attribute of a data has a weak influence on privacy weaknesses (dotted line). In some cases, the relevant categories for a component also determine the relevant categories for another component through *category-category* links. For example, the disclosure of personal data to unauthorized actors may cause the data subject embarrassment, loss of reputation or dignity. Hence, the *category-category* link between feared events and harms in Figure 1. Considering the multi-dimensional nature of privacy, it is also necessary to take into account *external factors* such as social and legal norms (*norms* in Figure 1) which can have an impact on certain attributes or categories of components.

The value assigned to an attribute can be 1) qualitative (e.g., using a fixed scale such as {low, medium, high}), 2) quantitative, either from a fixed set of options or from an unbounded set of values (e.g. natural or real numbers) or 3) descriptive. Examples of measurement scales can be found in [6, 8, 19, 20, 21].

The PRIAM methodology consists of two phases: the *Information gathering phase* and the *Risk assessment phase*. The first phase consists in gathering all the relevant information. The main difficulty for the analyst at this stage is not to overlook any factor that could have an impact on privacy risks. The component categories and lists of attributes are useful to this respect. The determination of the categories and attributes of one component may depend on those of other components as shown by the links in

[3]Note that the system component system does not have any category because it is the input of the analysis.

[4]Square corner boxes.

[5]Rounded corner boxes.

[6]We do not show these links explicitly in Figure 1 to avoid an over-crowded diagram.

Figure 1. The characterization of the components can be done by the analyst in any order compatible with these dependencies. The second phase (risk assessment) uses the values of the attributes to compute the risk levels, which are pairs (severity, likelihood), for each privacy harm. This computation is based on *harm trees* which are used to establish a relationship among privacy weaknesses, feared events and harms. The details of each of these phases are presented in Section 3 and Section 4 respectively through a running example, introduced in Section 3.1.1.

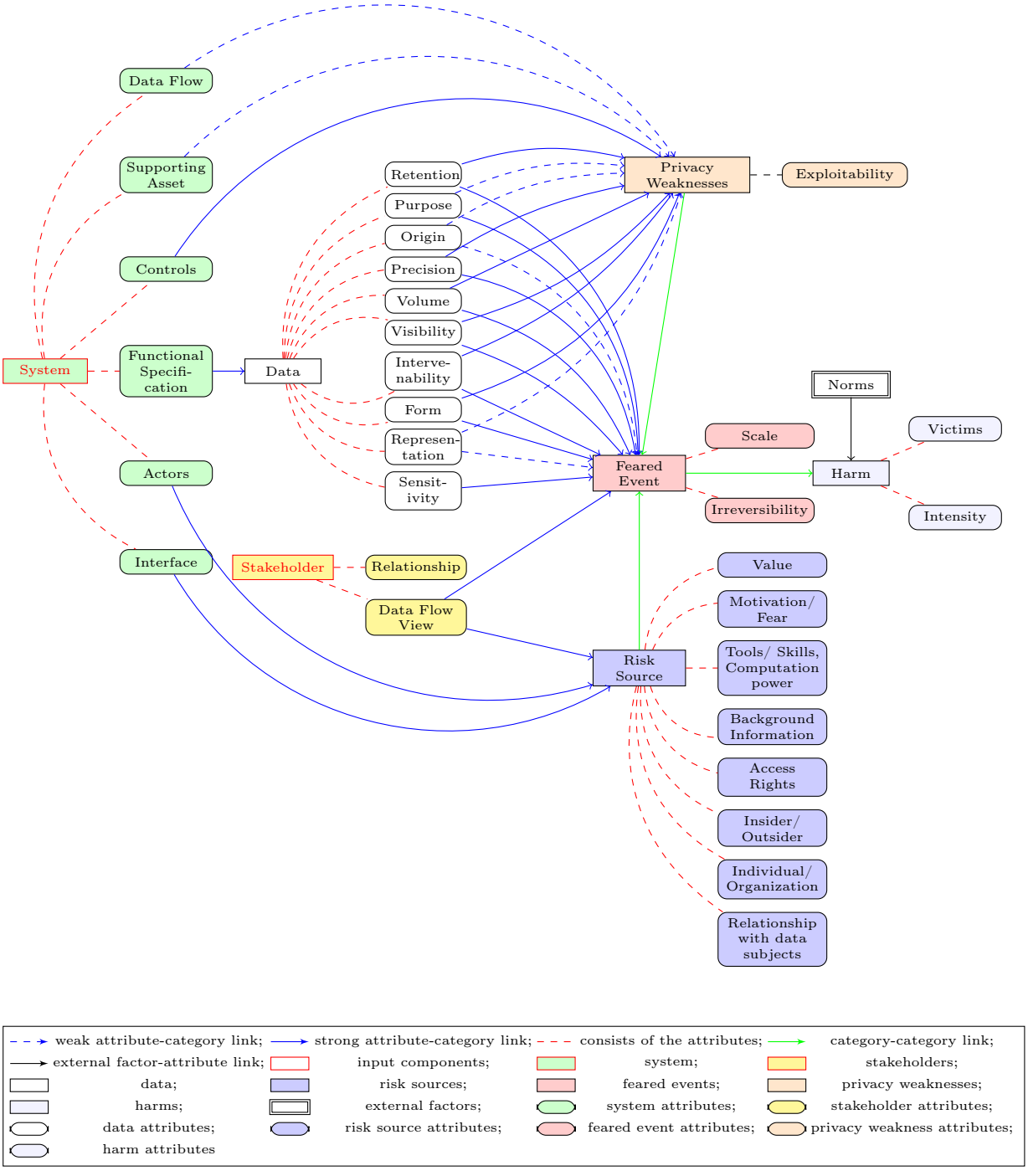


Figure 1: Information gathering phase for privacy risk analysis

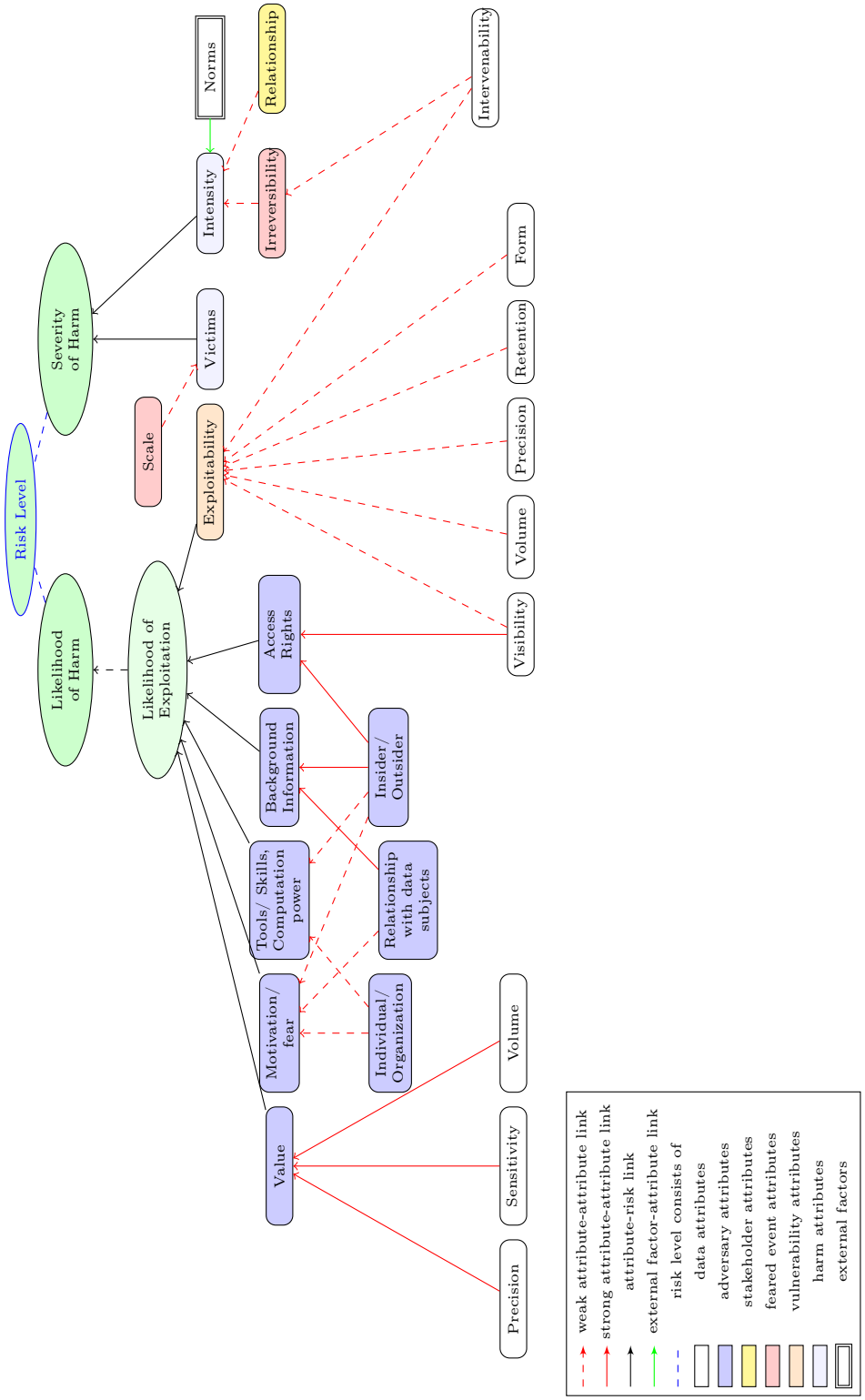


Figure 2: Attribute-attribute and attribute-risk links in privacy risk analysis

3 Information gathering phase

In this section, we describe the seven components to be considered (*system*, *stakeholders*, *data*, *risk sources*, *privacy weaknesses*, *feared events* and *privacy harms*) and a set of categories and attributes that should be used to define each of them. For ease of reading, we start the description of each component by a short definition and we illustrate it with a running example (introduced in Section 3.1.1).

We also discuss how the categories and the attributes of one component can be derived from those of the others. We refer to Figure 1 and Figure 2 for this discussion.

Where appropriate, we provide a simple scale or rule for measuring the values of the attributes of a component. It should be noted that these scales are merely suggestions and different choices can be made on a case-by-case basis.

3.1 Definition of the System

The starting point of the PRA is the detailed description of the system in terms of its attributes. The description plays a key role in the discovery of the categories and attributes of all other components. In this respect, the system can be considered as an input component for the PRA.

Definition 1 (System) *The system defines the logical boundary of the PRA. It should encompass the entire life-cycle of the personal data for the application (or set of applications) considered. It consists of various hardware and software components.*

Attributes. The following attributes should be used to describe the system:

1. The *functional specification* describing the global functionalities of the system (the services that it provides).

2. The *interface* including all interactions with the external world, with users and other systems. The possibility or not to collect the consent of the user should be defined by the interface component.

3. The *data flows* providing the internal view of the system, including sub-systems, their locations, the data they store or process, access rights to these data and the flows of the data among them. It is useful to represent the data flows in a system through a *data flow diagram (DFD)* which is a structured, graphical representation of the system based on four main types of building blocks: external entities, sub-systems, applications, data stores and data flows.

4. The *supporting assets* such as hardware, applications, data stores, software environment, etc.

5. The *actors* having access to the system or interacting with it, including their roles inside the organization of the data controller.

6. The *controls* consisting of legal measures (e.g., contracts between data controllers and third parties, between data controllers and data subjects, privacy statements and disclaimers of the data controller, Binding Corporate Rules (BCR), etc.), organizational measures (e.g., creating awareness among employees, training, incident management, information security policy and procedures, risk management, protection measures against thefts, vendor management, etc.) and technical measures (e.g., anonymization techniques, encryption schemes, access control and other privacy protection measures implemented in the system).

Depending on the time when the risk analysis is carried out, certain information may not be available and the characterization of the system may remain partial. For example, when the analysis is performed before the design of the system, only the functional specification, interface and actors may be available. Generally speaking, different frameworks (informal, semi-formal, formal) and levels of details can be provided at this stage. When only partial information is provided about the system, the analysis should be conservative (err on the safe side). Considering that the privacy risk analysis is a continuous process this initial information can be completed at a later stage.

3.1.1 Illustration: Definition of the FT System

To illustrate our framework, we use an example in the area of quantified self, which is chosen both because of its fast growth and for the various privacy risks that such systems may pose to their users [23,25,26,38,40]. Fitness tracker devices[7] allow their users to track their number of steps, strenuous activities, heart beats and location. They generally help users to log daily food intakes, set fitness goals, update weight changes, or participate in challenges. They also provide users different types of derived information such as sleep patterns, calories burnt, goals achieved, through a comprehensive dashboard. For the rest of this work, we consider a hypothetical fitness tracker (FT) inspired by existing products, but focusing on a subset of functionalities for conciseness. We first summarize these functionalities[8] followed by the other attributes of the system component: the interface, the data flows, the actors and the controls.

1. *Functional specification.* A fitness tracking system consists of the following subsystems:
   - *Tracking Devices* to collect fitness data such as number of steps or movements as the user walks, sleeps, runs, engages in strenuous activities and GPS data.
   - *Wireless Sync Dongle* to be used with a PC (by plugging to USB port) to enable wireless synchronization with tracking devices.
   - *Smart phone, PC* with wireless sync dongle attached to it are necessary to upload data collected by tracking devices to the User Management System. The user can access the User Interface through a PC or a smart phone (no dongle required).

[7] Fitbit(http://www.fitbit.com/home), Jawbone, Garmin are some examples.
[8] See Table 1 for a list of abbreviations.

- *Tracking System* embedded in tracking devices to store and manage collected fitness and location data till they are uploaded to the User Management System. It is responsible for encrypting data sent to the User Management System for syncing. It consists of the Tracking Application and the Tracking Data Store (for temporary storage of tracking data).
- *Tracker Connect System* to be installed in smart phone or PC (with respective versions, depending on the type of OS, etc.) by the user. It enables uploading of data from tracking devices to the User Management System, pairing tracking devices to the user account, updating contact lists in the Social Network Application (SNA) based on the phone contact list. It consists of the Tracker Connect Application.
- *User Management System* to store and manage all identification, contact, profile, location and fitness information of the user at the service provider's end. It consists of the User Data Store, the User Data Management Application, the Fitness Management Application and the Security Management Application.
  - New account and user ID creation and user profiles are handled by the User Data Management Application. It checks whether users have provided all necessary information to access the service and that a single tracking device is not attached to multiple accounts. It encrypts and stores all contact/identification and profile related user data in the User Data Store.
  - The Fitness Management Application receives all fitness and location information from the Tracker Connect System and stores them, after encryption, in the User Data Store. It uses different information provided by the user and the tracking devices to derive other fitness related information (calories burnt, sleep pattern, active minutes and distance covered) and keeps track of his progress (achievements with respect to goals set by the user). It provides this information to the User Interface to create a fitness dashboard for access by the user. This data is also encrypted and stored in the User Data Store. This application has no other security related functions.
  - The Social Network Application manages all contact lists, friend requests, messages sent to friends, participation in contests, comparison of fitness statistics with friends, etc. It stores all social networking related user data in the User Data Store. Data is encrypted before storage. This application has no other security related functions.
  - The Security Management Application has security related functions. Some of the security related functions interact with the user. These include management of privacy settings (visibility of user's data to other users), creation of new passwords, etc. Other security related functions are internal and do not interact with users. These include access control of information stored in the User Data Store by all other applications and

actors, checking for data integrity, key generation, distribution and management (storage, re-keying, deletion, etc.), secure storage of passwords, ensuring secure deletion of data, anonymization of data, etc.

- *User Interface* to enable users to interact with the system (access fitness dashboard and profile through user account, update profile information, set fitness targets, send messages to friends, participate in contests, etc.).

2. *Interface.* The contact with the user is established through User Interface, tracking devices, smart phones and PC.

3. *Data flows.* Data flows among major system components are depicted in Fig. 3. The TD, the WSD and the smart phone/PC are owned by the user. Each new user installs the TCS on his smart phone or PC. All other systems are located with the service provider and cannot be accessed by the user. The two main sources of data in this system are the users themselves and the tracking devices they own. The output data originates from the UMS. A new user creates an account with the service provider with his identification and contact information, through the UI over the Internet. The user is required to provide profile information (date of birth, gender, height and weight). He may also upload other information such as food logs and profile pictures to his profile. He may add friends to his social network and participate in contests, surveys and send messages to friends. The user can change the privacy settings of his account to make all or parts of profile information (such as height, weight, age, etc.), fitness related data (such as active minutes, sleep pattern, number of steps), location data and social network related data visible only to his friends or only to himself. By default, all such information is public. The UI communicates all data provided by the user for account creation and profile update to the UMS for storage and management. The UMS communicates user fitness related information to the UI. This information is displayed to the user in the form of a fitness dashboard. The User Interface also provides social network related information such as friend requests, list of friends/contacts, comparisons of activities with friends, challenges put forward by friends, etc. to the user. It also enables the user to search for a contact using e-mail ID and send friend requests, write messages, challenge his friends, etc. The TS installed in tracking devices communicate with the TCS installed in the smart phone or PC via Bluetooth Low Energy. For PC, a wireless sync dongle is necessary for the communication. The tracking device can automatically sync (real time or not) or sync when the user wants to. It can also send data to the Tracker Connect system in the live mode for the user to check his activities in real time using his PC or smart phone. The TCS receives instructions about tracking data retrieval from the UMS and forwards them to the TS. In response, the TS, after necessary authentication, sends its data to the TCS which then forwards the data to the UMS. However, in the live data mode, the data received is only displayed to the user via the Tracker Connect System but not sent to the User Management System. In all the above cases, encrypted data is sent after an authenticated channel has been established. The exceptional case is

the live data mode in which tracking data is not encrypted before communication.

4. *Supporting assets.* These are listed in Table 11 (Appendix A).

5. *Actors.* Users, administrators, service technicians (for addressing issues with tracking devices, wireless dongle), developers (for developing tracking products and proprietary applications), operators and other employees under the service provider.

6. *Controls.* Some important technical, organizational and legal protection measures taken by the service provider are described in Table 12 (Appendix A).

Abbreviations	Meaning
UMS	User Management System
SMA	Security Management Application
FMA	Fitness Management Application
UDMA	User Data Management Application
SNA	Social Network Application
UDS	User Data Store
TCS	Tracker Connect System
TCA	Tracker Connect Application
TS	Tracking System
TA	Tracking Application
TDS	Tracking Data Store
TD	Tracking Device
UI	User Interface
WSD	Wireless Sync Dongle

Table 1: List of Abbreviations

3.2 Definition of the Stakeholders

The term "stakeholder" is commonly used in the literature, generally without being defined. Even though its meaning may look obvious, we define it as follows to avoid any ambiguity.

Definition 2 (Stakeholder) *Any entity (individual or organization) to whom a piece of data relates to or who processes*[9] *or gets access (legally or not) to a piece of data at any stage of its lifecycle is referred to as a stakeholder.*

Categories. In addition to the three types of stakeholders (data subjects, data controller, data processor) set forth in the European Directive 95/46 [2] and GDPR [39], we consider third parties (any party other than the data controller operating the system and with whom the data subject interacts). Third parties can also be data controllers in the sense of the law (when they process personal data received from the main data controller

[9]Here we define "processing" in the same way as in the EU Directive. The EU Directive [2] defines processing of personal data as *"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."*

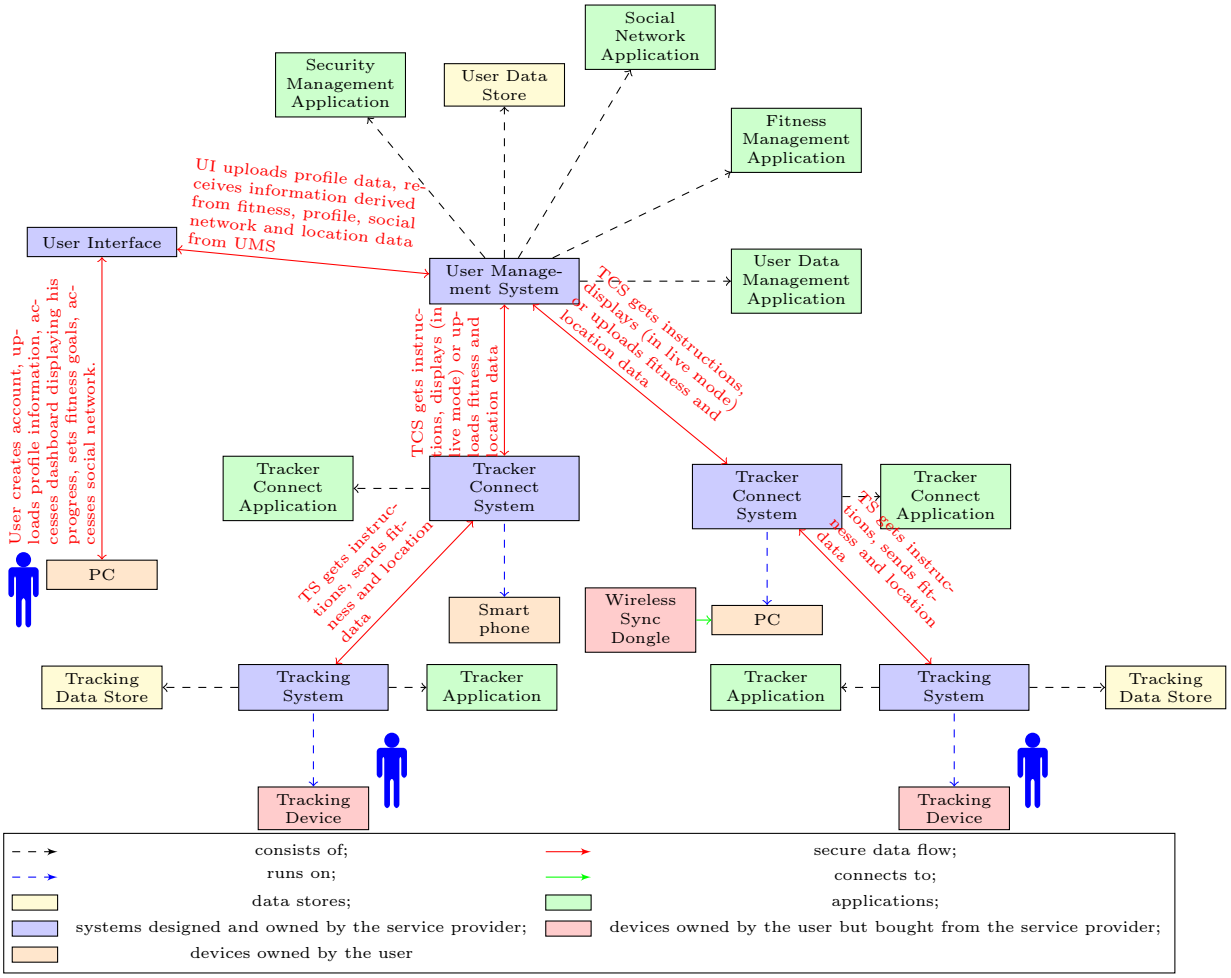


Figure 3: Data flow diagram for fitness tracking system

or from other subjects). For example, third parties receiving profile information about an internet user are third parties from the point of view of the user (who may even ignore their existence) but they are still data controllers in the sense of European Directive and the GDPR.

Attributes. Stakeholders should be described in terms of the following attributes:

1. The *data flow view* depicting how data flows across stakeholders. Data originates from the data subject and flows to the data controller. The flow may end at the controller, unless the controller delegates data processing to one or more data processors or third-parties receive the data from the controller (e.g., if the data controller sells the data to third parties, which then become data controllers themselves). Data processors may further give access to the data to sub-processors. Thus, data flow provides a complete view of all stakeholders who have access to the data. This data flow view should not be confused with the data flow described

in Section 3.1: it concerns data flows among stakeholders whereas the system definition (in Section 3.1) depicts flows of data within the system itself.

2. The *stakeholder relationships* (when such relationships exist) describing trust, hierarchical dependency, economic dependency, etc. among various stakeholders. The relationship of one stakeholder with other stakeholders can have an impact on privacy risks. Power imbalances often create difficult situations for the weaker party even if he is a victim of illegal or unfair practices. For example, when organizations with large user databases decide to change their privacy policy or their practices, then the user may suffer harms without being able to do much to remedy the situation. Any hierarchical relationship may have similar problems. In some long-lasting relationships it is possible to develop trust. For example, an individual who has been the customer of a bank for many years may decide to trust the bank based on his previous positive experiences with it. However, he may not trust another bank with whom he has only recently opened an account. Betrayal in a trusted relationship may also be more harmful to the victim as he may be caught off-guard, as compared to betrayal in untrusted relationships where more protective measures were employed from the beginning.

3.2.1 Illustration: Definition of the Stakeholder for the FT System

Categories. We consider three stakeholders for the FT system: the service provider (data controller), which is assumed to be the vendor of the device[10], the user (data subject) and third parties (which may receive de-identified data according to the privacy policy of the data controller as summarized in Table 12).
Attributes. Two attributes are associated with the stakeholders: the *data flow view* (which defines the flows of data between them) and the *stakeholder relationships*. We assume the following for the FT system:

1. *Data flow view.* Fitness, profile, contact, identification and location data flow from users to the service provider. Data derived from all other data flow from the service provider to users. Anonymized data may flow from the service provider to third parties.

2. *Stakeholder relationships.* The user can stop using the services associated with the FT system but cannot reuse his data with another service provider (lack of data portability). Therefore, the situation is slightly unbalanced (in favour of the service provider).

3.3 Definition of the Data

The personal data involved in the processing is also a key component to conduct a PRA.

[10]The risk analysis would be different if the service provider were the insurance company or the employer of the user.

Definition 3 (Personal Data [2, 7, 39]) *Personal data shall mean any information relating to an identified or identifiable natural person*[11] *and any information allowing such a person to be singled out or treated differently.*

The definition of personal data used here is mainly inspired by the definitions provided by the EU Data Protection Directive ("EU Directive" in the sequel) [2] and the GDPR [39]. The primary reason for this choice is that the EU provides a single, uniform definition which contrasts the multiple, competing attempts at defining PII in the US.
Categories. All personal data collected or more generally processed by the system should be considered. Data categories processed by a system are fully defined by the *functional specification* of the system. For example, if the functionality of the system (e.g., a smart grid system) is to provide consumers with detailed information about their energy consumption, then the system definitely processes energy consumption data. Similarly, if a system (such as smart phones) provides users with information about their GPS position, then these systems process location data. Both these systems also process identification and contact data of the user. The following non-exhaustive list of common categories of personal data can be a useful starting point to identify the relevant data for a given system:

- Identification and contact data (name, address, email address, etc.)
- Health data
- Genetic data
- Data providing information about personal life and relationships (sexual life, family life, social life)
- Data about origin
- Judicial data
- Data about personal beliefs (religion, political, philosophical, civil unions, etc.)
- Financial data
- Data about professional life
- Behavioural data (consumption habits, leisure, etc.)
- Location data
- Technical data (IP address, MAC address, URLs, etc.)

These categories of data are not exclusive and information of one category (e.g. location data) can be used to derive information of another category (e.g., behavioural information

[11] This person is the "data subject" defined in Definition 2.

or home address). This list should just be used as a checklist and source of inspiration to define the categories of data relevant for the system under study.
Attributes. Each data category relevant for the system under consideration should be described using the following data attributes:

1. Attribute related to the nature of the data
   (a) *Sensitivity*: whether the data is considered sensitive from the legal point of view[12].
2. Attributes related to the format of the data
   (a) *Form*: the data can be in raw form or pre-processed (encryption, biometric transformation, etc.).
   (b) *Precision* which depends on the type of data: e.g. granularity level of geolocation data, date or year of birth, etc.
   (c) *Volume*: number of data items collected per time period (e.g. every 15 minutes for electricity consumption).
3. Attributes related to the context
   (a) *Origin* describing the data source: explicit disclosure by the subject, implicit disclosure (e.g. collection of IP address, MAC address, video-camera pictures), disclosure by a third party (e.g. friend), creation by the controller (e.g. inference).
   (b) *Purpose*: the reason why the data is being processed by the system.
   (c) *Retention*: the period of time after which the data will be deleted.
4. Attributes related to control over data
   (a) *Visibility*: the set of actors who will have access to the data (who can at least read it).
   (b) *Intervenability* (inspired by [55]): possibilities for the data subject to exercise his rights (access, modification, deletion, challenge, etc.).

A detailed description of data being processed by the system using the above categories and attributes helps to determine potential privacy weaknesses and feared events. For example, if the *volume* of data collected is very high then there is a possibility of excessive data collection. Similarly, unencrypted data can be a potential privacy weakness. If the data subject is not allowed to update or modify incorrect data about himself (see the *intervenability* attribute) then there is a stronger risk that the data controller stores and uses inaccurate data. These links are further described in details in Section 3.5 and Section 3.6.

[12]For example, in the European context, the EU Directive [2] provides specific requirements for data that is sensitive and belongs to one of the following categories: health information, information about personal life, information about one's origin, information about personal beliefs. The GDPR [39] includes, in addition, biometric data and genetic data.

3.3.1 Illustration: Definition of the Data for the FT System

Categories. The FT system makes use of the following types of data:

1. Identification and contact data: name, e-mail address, physical address, user ID.
2. Profile information (associated with user ID): date of birth, gender, height, initial weight, stride length, pregnancy status, food log, profile picture[13], tracking devices (tracking device ID) associated with the user's account and fitness goals.
3. Social networking data: messages/challenges sent to friends, ranking of achievements (goals achieved, contests/challenges won, etc.) in comparison with friends, comments on discussion forum, contact list[14], etc.
4. Fitness information (associated with user ID): number of steps, movement information, weight updates, heart rate.
5. Location data: from GPS signals.
6. Information derived from tracking and profile data (associated with user ID): calories burnt, active minutes, floors climbed, distance travelled and sleep pattern.
7. Technical data: browser type, operating system, IP address, etc.

Attributes. For the sake of conciseness, below we describe the relevant attributes only for fitness data. In practice, the analyst must define relevant data attributes for all data types.

1. Attribute related to the nature of data:
   (a) *Sensitivity.* Not sensitive in Europe if considered as well-being data (and not health data).
2. Attributes related to the data format:
   (a) *Precision.* Collected one unit per user per time unit. More than one tracking device ID cannot be used at a point of time.
   (b) *Volume.* Tracking devices collect data every minute and store them for 7 days. Daily records can be stored for 30 days in TDS. Heart rate data is collected every second during running or exercising and at 5 seconds interval at other times. The data can be uploaded to the UMS every 15 minutes if the tracking device is near a PC or smart phone. Real time sync is also possible, if the option is enabled by the user. Otherwise, users may choose to upload data at any interval greater than this. However, if the interval is too big, some data will be lost.

[13] uploaded by user or obtained from other SNS if those credentials are used to create this account
[14] from contact list of phone or other SNS if those credentials are used to create this account

(c) *Form.* Encrypted and signed during storage and transmission, decrypted during processing. All systems and actors need to authenticate themselves to access the data.

3. Attributes related to the context

   (a) *Origin.* All fitness tracking information are required data, explicitly collected from users.

   (b) *Purpose.* All fitness related data are used for determining personalized fitness statistics for the customer such as calories burnt, distance travelled, sleep quality, weight lost, etc. De-identified data may be sold or shared with partners or public in different ways such as by providing research reports on health, fitness, etc. This data may also be used for research to improve products and services.

   (c) *Retention.* De-identified data is retained even after the user stops using the service. Identifiable data is retained for the time the user uses the service.

4. Attributes related to the control

   (a) *Visibility.* Visible to the user and the UMS administrator. Other users registered as friends of the user in the SNA may also be able to see this data depending on privacy settings used by the user.

   (b) *Intervenability.* None. All fitness data are available for downloading by the user from the user account.

3.4 Definition of the Risk Sources

The literature often refers to the adversary or the attacker. But, here, we prefer to use the term "risk sources" as it is less security connotated and is not limited to malicious actors.

Definition 4 (Risk source) *A risk source is any entity (individual or organization) which may process (legally or illegally) data belonging to a data subject and whose actions may directly or indirectly, intentionally or unintentionally lead to privacy harms.*

Categories. The categories of risk sources to be considered are: insiders (eg., system administrator, employee), outsiders (eg., users of the system), the data controller itself, governments and law enforcement bodies, criminals and other organizations. These categories can be derived from *actors* and *interface* attributes of the system, the *data flow view* attribute of the stakeholders and the categories of data involved. The *actors* attribute specifies various roles in the organization of the data controller that may act as risk sources. The *interface* attribute determines the contact points between the system and the external world and hence helps identifying the potential risk sources outside the system, such as hackers, friends, acquaintances or family of data subjects, etc. The *data flow view* identifies different stakeholders that handle the data and enables to identify

stakeholders such as third parties, other data subjects, data processors and data controllers themselves as potential risk sources. There may be overlaps in the usefulness of the categories by the attributes (for example third parties may be identified both through the *interface* and the *data flow view* attributes), but this redundancy reduces the risk for the analyst to overlook any potential risk sources.

Attributes. Each risk source must be described using the following attributes:

1. The *relationships* between the risk sources and different stakeholders
   (a) *Insider / outsider* describing whether the risk source works within the data controller organization or not.
   (b) *Individual / Organization* describing whether the risk source acts as an individual or as an organization.
   (c) The *relationship with data subjects* describing trust relationships between risk sources and data subjects. For example, a friend or a family member is usually trusted by the data subject, whereas limited trust is placed on the service provider or a service technician.
2. Level of motivation
   (a) *Value* describing the potential value of the privacy breach for the risk source (e.g., financial benefit, retaliation, thrill, etc.).
   (b) *Motivation / fear* describing all incentives and dis-incentives (e.g., risk of being caught) for the risk source.
3. Resources
   (a) *Background information* describing additional information available to the risk source which may help it to carry out a privacy breach (e.g., detailed knowledge of the system, security flaws, etc.).
   (b) *Access rights* to different types of data being processed by the system (for e.g., a system administrator may already have access to some data whereas other employees do not).
   (c) *Tools / skills, computation power* available to the risk source.

As shown in Figure 2, the values of some of the above attributes such as *insider / outsider*, *individual / organization* and *relationship with data subjects* can influence the values of other attributes such as *background information*, *motivation/fear*, *access rights*, etc. The fact that the risk source is an *insider or outsider* can strongly determine whether it possesses *access rights* to personal data, *background information* and also influences the nature of *tools/skills or computation power* it possesses and its possible motivation/fear. A system administrator in charge of a critical sub-system can be assumed to have extensive knowledge about the system including its weaknesses and may have been given access rights to personal data processed by the system. However, being in such a responsible position, he may be subject to constant scrutiny (possibly at a

higher level than other employees) and hence, expect high chances of getting caught and fear losing his job and other severe punishments if he tries to exploit a privacy weakness. Similarly, a risk source's *relationship with the data subject* strongly determines the *background information* he has and also influences his *motivation/ fear*. For example, a close family member or a friend may be able to easily elicit hints about the password the data subject uses to access a system or may possess detailed information about the data subject (such as personal habits, usual locations, etc.) that can enable him to easily re-identify anonymized data. If the risk source is an *organization* (such as a third party), it may have high financial motivations to re-identify anonymized data to utilize it for its own business purposes. For example, a health insurance provider may want to identify all its users who have unhealthy lifestyles from fitness data it buys from a fitness tracking service so that it can increase insurance premiums. Risk sources backed by an *organization* will also generally have higher financial and technical resources and hence possess better tools/skills and computation power than *individual* risk sources.

The *value* of a privacy breach for a risk source is influenced by the data attributes *precision*, *sensitivity* and *volume*. Sensitive data such as financial data, health data definitely have more appeal to a risk source. Similarly, high volume and precision data may be attractive to a risk source because of the possibilities of data inference that they provide.

As discussed before, it may be possible that there are overlaps among the determinants or influencers of different attributes of the risk sources, which is useful to ensure that important factors are not overlooked during the analysis.

3.4.1 Illustration: Definition of the Risk Sources for the FT System

Categories. We consider eight main risk sources for the FT system (see Table 2).
Attributes. Table 2 provides the values of the relevant attributes for each risk source. The values of some of these attributes (such as *value* and *motivation/ fear*) may depend on the particular exploitation but in Table 2 we have assumed pessimistic values. In practice, these values should also be assigned by the privacy expert. For this use-case, risk source capability is measured using the following scale:

1. *High* if most attributes favour an exploitation;
2. *Medium* if only some of the attributes favour an exploitation;
3. *Low* if very few attributes favour an exploitation.

Code	Categories	Individual / organization	Insider / outsider	Value of exploitation[15]	Motivation / Fear	Background information	Access rights to personal data	Tools / Skills, Computation power	Relationship with data subject

[15]Financial benefit, thrill, revenge, etc.

A.1	Service provider	Organization	Insider	High	High	Extensive system knowledge	All data	High	Semi-trusted
A.2	Rogue UMS administrator	Individual	Insider	High	Medium	Extensive UMS and general system knowledge	All data	Medium	None
A.3	Rogue UMS operator	Individual	Insider	High	Medium	Moderate UMS knowledge, moderate general system knowledge	Contact/ identification data	Medium	None
A.4	Rogue employee[16]	Individual	Insider	High	Medium	Publicly available data	None	Low	None
A.5	Hacker	Individual / organization	Outsider	High	High	Publicly available data, good general system knowledge	None	High	None
A.6	Friend or family	Individual	Outsider	Medium	Low	Publicly available data, some knowledge about user's personal life	Identification/ contact data	Low	Trusted
A.7	Third party	Organization	Outsider	High	High	Publicly available data, some knowledge about the user	Derived data	High	None
A.8	Service technician	Individual	Intsider	Medium	Low	Publicly available data, some knowledge about the user, good knowledge of TD	Identification/ contact data	Medium	Semi-trusted

Table 2: Some relevant risk sources in the FT system and their attributes

3.5 Definition of the Privacy Weaknesses

As in the previous section, we prefer to use a more general term than vulnerabilities here and use "privacy weakness" in the following sense:

Definition 5 (Privacy weakness) *A privacy weakness is a weakness in the data protection mechanisms (whether technical, organizational or legal) of a system or lack thereof that can ultimately result in privacy harms.*

Categories. Privacy weaknesses include: 1) weaknesses introduced by design choices or choices of functionalities; 2) system design errors and 3) implementation errors. Privacy weaknesses due to implementation errors or design flaws are akin to vulnerabilities in traditional computer security. Privacy weaknesses due to design choices or the definition of the functionalities of the system itself are specific to privacy. Typically, the excessive collection of data can be a deliberate choice (either at specification time or at design time) to accumulate data that could be exploited in the future. In the sequel, we refer to security vulnerabilities as implementation errors causing deviations of an application from its intended security-related functions. Functional errors refer to implementation errors causing deviations of an application from its intended core functions.

As shown in Figure 1, the relevant privacy weaknesses are determined by the values of system attribute *controls* and data attributes *retention*, *form*, *precision*, *intervenability*, *visibility* and *volume*. They are also influenced by other system attributes *supporting*

[16]Other than system administrator, service technician, operator.

assets and *data flow* and data attributes *origin*, *purpose* and *representation*. These attributes help in finding the weaknesses in the data protection mechanisms. The system attribute *controls* which constitute the legal, technical and organizational protection measures implemented by the service provider provide information about the strength of the data protection mechanisms already in place. It is therefore a major determinant of the privacy weaknesses of the system. The privacy policy followed by the service provider and the access control measures in place can also reveal all indicate potential privacy weaknesses. Similarly, the *form* of the data, i.e., whether it is encrypted or not during transit, storage or during computations is an indicator of a privacy weakness. Unnecessarily long data *retention* periods, high *precision* and *volume* of data, and excessive *visibility* of data may increase the possibility of exploitations of the data. On the other hand, if the data subjects have good *intervenability* on their data, then many misuses can be addressed. The *flow* of energy consumption data outside the premises of the data subject, for example, in the case of smart metering, increases the possibility of privacy weaknesses. If such data was stored only in the consumer's premises, then many risk sources such as data controllers and actors within the data controller's organization would not have access to it. These attributes also determine the category to which each privacy weakness belongs. For example, if the data controller has already implemented strong encryption schemes and robust keying and cryptographic parameter selection mechanisms for secure data storage, then a privacy weakness in data storage results from an implementation error (e.g., software error) rather than a design error. Similarly, if the data controller has chosen to use a weak encryption scheme for data storage, then the resulting privacy weakness in data storage is a design error (i.e., choice of poor encryption scheme) rather than an implementation error.

Attributes. We consider only the *exploitability* attribute for privacy weaknesses. *Exploitability* denotes how easy it is to exploit a particular privacy weakness. It is established based on the definition of the system and influenced by data attributes *form*, *retention*, *visibility*, *volume*, *precision* and *intervenability* (see Figure 2). For example, data in unencrypted *form* or data with a long *retention* period without sufficient protection or data with high *visibility* is more likely to suffer from unauthorized access. Similarly, data of high *precision* and *volume* can be more easily used for the purpose of data interference. On the other hand, high *intervenability* can prevent unauthorized modification or retention of erroneous data.

3.5.1 Illustration: Definition of the Privacy Weaknesses for the FT System

Categories. Various privacy weaknesses of different categories are shown in Table 3. For this use case, example of functional errors include erroneous computation of fitness statistics such as calories burnt or active minutes by the FMA, or sending friend requests on the phone contact list by SNA without the user prompting such requests. The SMA has security as its core function. So, SMA errors refer to errors in security-related functions such as key generation or access control. Security vulnerabilities also include failures of applications such as FMA or SNA to properly encrypt data before storage.

Attributes. Table 3 shows *exploitability* values of some relevant privacy weaknesses of

the FT system. We assume the following definitions:

1. *Low* means difficult to exploit (for e.g., the associated data is encrypted, not visible to many actors or properly de-identified, the concerned supporting assets are difficult to access by risk sources);

2. *Medium* means exploitable with moderate difficulty (e.g., the associated data is unencrypted but is of low volume and precision or not properly de-identified, the concerned supporting assets are moderately difficult to access by risk sources);

3. *High* means easily exploitable (e.g., the associated data is unencrypted, is of high volume or precision, not de-identified at all, the concerned supporting assets can be very easily accessed by risk sources, associated data is visible to risk sources, no possibilities of intervention by data subject, etc.).

The values are assumed to be assigned by a privacy expert.

Code	Privacy Weaknesses	Exploitability
V.1	Unencrypted data processing[17]	Medium
V.2	Unencrypted fitness and location data transmission in live mode	Medium
V.5	Insufficient system audit	High
V.6	TD responds to broadcasts from other bluetooth devices in range	Medium
V.7	TD does not change its private address	Medium
V.8	TCS reports private address to UMS	Medium
V.9	Weak anonymization of data	Medium
V.10	No manual control of pairing between TD and smart phone	Medium
V.11	Unencrypted log of communication between TCS and UMS stored in smart phone/PC.	Medium
V.12	Security vulnerability in FMA	Medium
V.13	Functional errors in FMA	Low
V.14	Functional error in SMA	Medium
V.15	Security vulnerability in UDMA	Medium
V.16	Security vulnerability in TCA	Medium
V.17	Functional errors in TCA	Low
V.18	Functional errors in TA	Low
V.19	Security vulnerability in TA	Medium
V.20	Security vulnerability in UI	Medium

[17]Here, by processing, we do not consider storage and transmission.

V.21	Non-enforcement of strong passwords for account access	Medium
V.22	Not prohibiting re-identification through contracts with third parties	High
V.23	Not binding third parties to maintain appropriate level of data protection	High
V.24	Default privacy setting is "public" for all data	High
V.25	Security vulnerability in SNA[18]	Medium
V.26	Functional error in SNA[19]	Medium
V.27	Lack of data minimization	High

Table 3: Privacy weaknesses in the FT System and their exploitability [16, 18, 42, 54].

3.6 Definition of the Feared Events

We introduce a distinction between feared events which are "technical events" and privacy harms (defined in the next section) which correspond to the impact of feared events on people.

Definition 6 (Feared Event) *A feared event is an event of the system that occurs as a result of the exploitation of one or more privacy weaknesses and may lead to privacy harms.*

Categories. Examples of categories of feared events that an analyst should consider include:

- Excessive data collection (e.g., collection of energy consumption data by smart meters every 15 minutes without consumer consent).
- Unauthorized access to data[20] (e.g., access to data by hackers).
- Unauthorized modification of data (e.g., modification of energy consumption data by the service provider).
- Use of data for unauthorized purposes [21] (e.g., use of fitness data by the data controller to build detailed user health risk profiles) and unjustified data inference or re-identification (e.g., inference about one's sleeping patterns or cooking habits from energy consumption data).

[18] For e.g., not encrypting social network data before storing in the UDS.
[19] For e.g., sending friend requests to people in the phone contact list without the user prompting such requests.
[20] This includes any use of data by the entity which gains unauthorized access to it.
[21] This includes only the use of data for unauthorized purpose by the data controller or anyone who has been authorized by the data controller to have access to the data.

- Storage or use of inaccurate data (e.g., not providing consumers ability to update, modify, correct or challenge incorrect or outdated data about himself).

- Disclosure of data to unauthorized actors or unauthorized publication (e.g., data controllers giving access to data to third parties without data subject's consent).

- Retaining data more than necessary (including lack of deletion or ineffective deletion).

As shown in Figure 1, feared event categories are determined by the privacy weaknesses of the system. Therefore many of the attributes that determine privacy weaknesses also contribute in the determination of feared events. Since conceptually, feared events are more related to the data than to the system itself, as compared to privacy weaknesses, we assume that system attributes do not play a role in determining feared events. The data attributes *retention*, *purpose*, *precision*, *volume*, *visibility*, *intervenability*, *form* and *sensitivity* and the stakeholder *data flow view* attribute determine feared events. Feared events are also weakly influenced by the data attributes *origin* and *representation*. For example, the *data flow view* reveals whether the data controller has the possibility to disclose any data to third parties (with or without consent, with or without proper protection measures). Similarly, the *volume* of data collected for a particular *purpose* indicates whether excessive data collection is taking place. Along with *precision*, it also reveals whether there is a possibility of excessive data inference.

Attributes. For each feared event, the following attributes must be considered.

1. *Scale.* It measures the number of potential individuals whose personal data is concerned by a feared event. This is not to be confused with the victims attribute of the harm component. In many cases, the number of victims of a feared event is smaller than the number of victims of the corresponding harm. For example, the unauthorized access to genetic data not only affects the specific individual (who is the victim of the feared event) whose data has been exposed but also his family members (who are all possible victims of harms caused by the feared event). Similarly, behavioral trends observed for a small group of individuals (victims of the feared event) of a particular religion or ethnicity may often be generalized for all individuals (victims of the harm) belonging to the same group.

   Depending on the actual exploitation or risk source, the scale of a feared event may vary. For example, a rogue system administrator may either decide to target one consumer and reveal his personal data or he may provide unauthorized access to data belonging to many consumers. In the former case, only a single individual is affected whereas in the latter many consumers are affected. For simplicity, we consider only the most likely scenarios for each feared event. For example, the data controller is more likely to practice excessive data collection for all its consumers rather than target only a single or consumer.

2. *Irreversibility.* For a single individual, irreversibility denotes the difficulty with which the feared event can be reversed.

Two main factors influence irreversibility: the extent of exposure of the personal data and the technical difficulty to reverse the consequences of feared event for a data item. The second factor depends on the *intervenability* attribute of the data (see Figure 2). For example, if the sleeping pattern of an individual is leaked to the public, then this data is available to many third parties, making complete deletion impossible in practice. The settings of a social networking site may be poorly designed thus becoming a technical obstacle for an individual who wants to remove an embarrassing information about him posted by a friend.

As with scale, the value assigned for irreversibility for a feared event depends on the particular exploitation and risk source. Here, for simplicity, we consider the most likely value for each feared event.

Irreversibility	Extent of exposure of data due to a feared event	Technical difficulty to reverse the effect of a feared event
Low	Low	Low
Low		Medium
Medium		High
Low	Medium	Low
Medium		Medium
High		High
Medium	High	Low
High		Medium
High		High

Table 4: Measurement rule for reversibility of feared events

3.6.1 Illustration: Definition of the Feared Events for the FT System

Categories. The most relevant feared events and their attributes for the FT System are presented in Table 5.

Attributes.

1. *Scale*: Public data disclosure may happen for some, but not all users[22], leading to a 'medium' value [26]. However, if the data controller discloses data intentionally to third parties it may do so for all users. So, we assume the most pessimistic values here.

2. *Irreversibility*: It may be difficult to remove all traces of fitness data once disclosed to the public [26]. Some relevant feared events for the FT system (determined from privacy weaknesses and risk sources as shown in Figure 1) and their attribute values are given in Table 5.

We assume the following values for the *scale* attribute:

[22] since, not all users use their default privacy setting

1. *Low* when only a single or very few individuals are affected.
2. *Medium* when many individuals are affected.
3. *High* when all individuals are affected.

For the *irreversibility* attribute, we assume the values shown in Table 4.

Code	Feared events	Relevant scenarios	Scale	Irreversibility
FE.1	Excessive collection of fitness data	Collection of user's fitness related data at a higher volume or precision than the user consented for	High	Medium
FE.2	Use of fitness and identification data for unauthorized purpose	Targetted advertising, sending invitation for clinical trials	High	Medium
FE.3	Excessive[23] data inference from fitness and profile data	Health risk profiling	High	High
FE.4	Disclosure of identifiable fitness related data[24] to unauthorized actors or public	Publication of sleep patterns online, selling user health profiles to employers or data brokers without user consent	High	High
FE.9	Unauthorized access to data	Criminals get access to fitness data	Medium	High

Table 5: Feared events and their attributes

3.7 Definition of the Privacy Harms

Privacy harm assessment is the ultimate goal of the analysis. The notion has been exclusively studied by lawyers [15, 49] but has received less attention from computer scientists. We consider the following definition:

Definition 7 (Privacy Harms) *A privacy harm is the negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events.*

Categories. The relevant privacy harms are derived from the feared events and external factors such as societal norms, legal environment, etc. (see Figure 1). The following categories of harms have been identified in previous works [15, 17, 47, 48, 49] and should be considered in the PRA:

1. *Physical harms* such as physical ailments, death, injury, etc. For example, a criminal may stalk and injure an individual after coming to know his precise location every evening from check-ins posted by the individual on a social networking site.

[23] By using the fitness tracking devices, the user agrees to some data inference which shows him the calories he burned, his active minutes, etc. Here, "excessive" refers to any inference that is done beyond the expected functionality, which means without user consent.

[24] By fitness related data, we mean any fitness data collected by the tracking device or any data inferred with or without user consent from fitness, profile and location data.

2. *Economic or financial harms* such as loss or damage of property, unanticipated financial loss, etc. Burglars having access to energy consumption data may infer when the occupants are not at home or if the home security system is inactive or not installed.

3. *Mental or psychological harms* constitute fear of misuse of personal data, fear of being observed, fear of being treated unfairly, anxiety, mental distress, etc. For example, a potential employer may turn down a a job application to a consumer because of alleged unhealthy lifestyle inferred from his fitness data.

4. *Harms to dignity or reputation* include embarrassment, humiliation, etc. For example, disclosure of intimate personal habits or unhealthy lifestyle to colleagues or the public may cause him embarrassment.

5. *Societal or architectural*[25] *harms* such as the sense of being always observed, chilling effect or loss of creativity affecting the society due to constant monitoring by government, law enforcement bodies or private companies. Remote switching off of energy supply during periods of high demand may also deprive consumers of utilities which are essential for leading a normal life.

Attributes. The following attributes should be considered for each harm:

1. The *victims of the harm* which may belong to the following categories: 1) individual data subjects; 2) specific groups of data subjects based on age, gender, religion, ethnicity or profession, etc. and 3) society. It is influenced by the *scale* attribute of the feared event (see Figure 2).

2. The *intensity* of a harm expresses the various effects of a harm on the victims. It depends on factors such as the duration of the harm or the extent of damage caused. It is also influenced by the *irreversibility* of the corresponding feared event, the *stakeholder relationships* and external factors such as societal norms (see Figure 2). If a feared event has high *irreversibility*, then its impact on the victim is more intense than if it has low irreversibility. Similarly, weaker power positions of data subjects with respect to data controllers may make it more difficult for data subjects to have the harm stopped or addressed, thus increasing the intensity of the harm.

3.7.1 Illustration: Definition of the Harms for the FT System

Categories. For the FT system, we consider the following categories of harms:

1. *Physical harms.* A user may be stalked and injured when a criminal uses his location data.

[25] In the literature on privacy harm, some scholars [15, 17, 47, 48, 49] claim that privacy harms not only affect individuals, but the society at large. It is then sometimes referred to as *"architectural harm"*. For example, persistent monitoring and social control can lead to chilling effect and lack of creativity and in the long run impede civic life, artistic and technological innovations [15].

2. *Financial harms.* A user may have to pay higher health insurance premium for his alleged sedentary lifestyle inferred from fitness data.

3. *Psychological harms.* A user may suffer from mental distress when denied a job based on his alleged unhealthy lifestyle inferred from fitness data.

4. *Harms to dignity or reputation.* A user may be embarrassed if his personal activities are publicly disclosed.

Attributes. The harm attributes can be described as follows:

1. *Victims*, may be: a) individual data subjects; b) groups of data subjects (e.g., increased health insurance premium may affect some users of certain age, see Table 8).;

2. *Intensity.* Increased health insurance premium has long term financial effect and so is of high intensity (see Table 8). The severity of harms is discussed in the next section.

The attribute *victims* is measured using the following scale:

1. *Low* when only specific individuals and their families are affected.

2. *Medium* when individuals belonging to a group (age, gender, religion, ethnicity, origin, profession) are affected.

3. *High* when society is affected.

The *intensity* attribute is measured using the following scale (inspired from [20, 21]):

1. *Low* when the victim faces very few consequences of the harm, the consequences are easily reversible and do not last for a long time.

2. *Medium* when the consequences of the harm can be reversed with some difficulty and lasts for a certain length of time.

3. *High* when the victim faces significant consequences of the harm, the consequences cannot be reversed at all or can be reversed with great difficulty and they last for a long time.

Table 6 shows some intensity values for different types of harms.

Intensity	Examples of harms
Low	Receipt of unsolicited mails, targetted advertising
Medium	Undesirable disclosure of intimate personal habits to friends, stalking
High	Increased health insurance premium, denial of a job, undesirable disclosure of intimate personal habits to the public

Table 6: Intensity of Harms

Based on the values of the attributes victim and intensity, the severity of each harm can be evaluated as shown in Table 7.

Severity	Victims	Intensity
Negligible	Low	Low
Limited		Medium
Significant		High
Limited	Medium	Low
Significant		Medium
Maximum		High
Significant	High	Low
Maximum		Medium
Maximum		High

Table 7: Harm severity evaluation

Harm	Example of event	Categories	Victims	Intensity	Severity
H.1	Undesirable disclosure of intimate personal habits to the public [25, 26]	Psychological, harm to dignity	Low	High	Significant
H.2	Increased premium for health insurance [38]	Financial	Medium	High	Maximum
H.3	Undesirable disclosure of intimate personal habits to friends[26]	Psychological, harm to dignity	Low	Medium	Limited
H.4	Denial of a job due to inferred health problems [40]	Psychological, financial	Low	High	Significant

Table 8: Harms in the FT System and their attributes

4 Risk Assessment Phase

When the information gathering phase is completed, the second phase which is the risk assessment phase itself, can start. A harm may result from one feared event or combinations of different feared events. For example, health insurance premium can be increased if the service provider infers potential health problems from the user's fitness data and discloses this information to insurance providers or if unauthorized access to fitness data takes place. Similarly, a feared event may result from the exploitation of one privacy weakness or a combination of different privacy weaknesses and different risk sources. Risk sources may get access to data if data is stored, processed or transmitted without encryption or if the access control implementation is poor. The exploitation of a given privacy weakness may contribute to the recurrence of multiple feared events. For exam-

[26]It includes disclosure of personal activities to friends who are not on the user's social network or undesirable disclosure of activities that are too personal to friends on the social network.

ple, if the service provider does not enforce sufficient system audit, then it will be easier (because it is likely to remain undetected) to collect excessive data, use it for unauthorized purposes or disclose it to unauthorized actors. A natural way to express these relationships among harms, feared events and privacy weaknesses is through harm trees. Harm trees are akin to attack trees in computer security [4, 12, 14, 27, 28, 41, 43, 44, 45, 46, 53]. The use of this type of trees is not new for privacy, even if very few papers have been published on this topic. In [22], Deng et al. use threat trees to link what they define as threats to vulnerabilities in a system. Similarly, Friginal et al. [24] describe attack trees to link what they define as adverse impacts (e.g., disclosure of the nearest friends of an user) to attack scenarios (e.g., hacking a device). However, these works do not provide an end-to-end link between privacy harms and exploitations of privacy weaknesses as described here.

4.1 Construction of Harm Trees

The root node of a harm tree denotes a harm. Leaf nodes represent privacy weaknesses exploited by the most likely risk source for the particular harm and represented by pairs (privacy weakness, risk source)[27]. The tree is structured in branches leading to the harm. Feared events are connected by an AND node if all of them are necessary to lead to the harm. On the other hand, if any one of several feared events lead to a harm then they are connected by an OR node. Similarly, the exploitation of privacy weaknesses leading to a feared event are connected by an AND node if all such exploitations must happen in order for the feared event to take place. When any one of a set of privacy weaknesses is sufficient to lead to a feared event then they are connected by an OR node. Harm trees can be used not only to compute the likelihood of harms but also to identify the privacy weaknesses that have to be addressed to reduce the risk to an acceptable level.

4.1.1 Illustration: Construction of harm trees for the FT System

Figure 4, Figure 5 and Figure 6 respectively show the harm trees for the three harms "disclosure of intimate personal habits to the public (H.1)", "increased health insurance premium (H.2)" and "disclosure of intimate personal habits to friends[28] (H.3)" in FT. H.3 includes the disclosure of personal habits to friends who are not members of the user's social network or undesirable disclosure of habits that can be considered as too personal (how many times the user wakes up during the night, how long he sleeps, what unhealthy food he indulges in, recent weight gains, pregnancy status, etc.) to friends on the social network. As shown in Table 8, disclosure to friends and the public may have very different effects, at least in terms of intensity. The harm trees in Figure 4 and Figure 6 also show that they may take place in different ways (i.e., by the exploitation of different privacy weaknesses by different risk sources).

[27] Strictly speaking, a harm tree should be associated with a set of risk sources. This set can be a singleton in case of individual risk source or denote a group of risk sources, who may be colluding or not, depending on the interactions needed to exploit the privacy weaknesses.

[28] While computing risks, we assume that the friend is not a hacker.

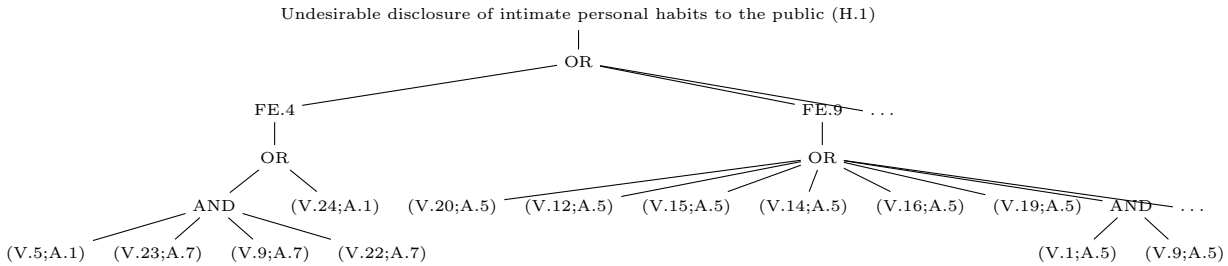


Figure 4: Harm tree for the undesirable disclosure of intimate personal habits to the public (H.1)

H.1 may result from the disclosure of identifiable personal fitness related data to the public due to default privacy setting "public" or because the data controller decides to publish poorly de-identified data without taking sufficient measures to stop third parties who get access to such data from re-identifying them. It may also result from unauthorized access by hackers to data by exploiting various privacy weaknesses in the system (such as processing of unencrypted, poorly anonymized data, security vulnerabilities in the UMS) who then release this data to the public.

H.2 (increased health insurance premium) can result from the service provider selling to health insurance providers data (e.g., health risk profiles) derived from fitness data by excessive inference without proper de-identification (see Figure 5). We assume that the health insurance provider itself is very unlikely to access fitness data unscrupulously (i.e., either exploit privacy weaknesses itself to access the data or simply buy it from unscrupulous actors such as hackers or malicious insiders who have access to the data). Here, we assume that the user has not been informed about the possibility of such uses of his fitness data. Hence, the increased health insurance premium due to a health risk profile generated from his fitness related data is unanticipated by the user. However, it should be emphasized that this analysis is very much dependent on our assumptions about the FT System. If the provider of the FT System were the health insurance provider of the user and health insurance is one of the purposes of the processing, then increased health insurance premium is not necessarily a harm.

H.3 can happen because of the disclosure of identifiable personal fitness data to friends not members of the social network due to default privacy setting of "public" or because of unauthorized access to data by friends (in the social network or outside it) by exploiting various privacy weaknesses (such as poor passwords, security vulnerability in TCA, etc.).

4.2 Risk level assessment

As usually done in the IT security area, the risk level for a privacy harm is determined as the pair: (severity, likelihood). The severity assessment for the FT System was described in Section 4.2.2. We describe the computation of the likelihood of harm in Section 4.2.1 and apply it to the FT System in Section 4.2.2.

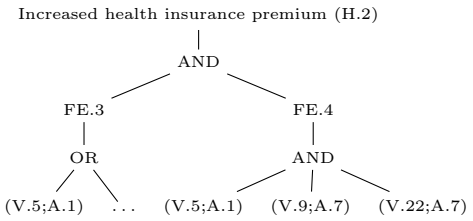


Figure 5: Harm tree for increased health insurance premium (H.2)

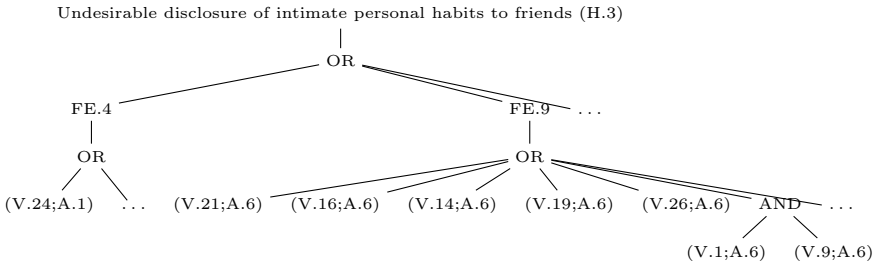


Figure 6: Harm tree for the undesirable disclosure of intimate personal habits to friends (H.3)

4.2.1 Computation of likelihood

The likelihood of a harm is the probability of the occurrence of the harm. It depends on the likelihood of the feared events which can be computed on the basis of the harm trees. A harm tree may involve several risk sources. This is specially true in cases of unauthorized access to data where such access may be gained by different risk sources such as hackers or rogue system administrators. Therefore, the exact risk source depends on the precise conditions of the occurrence of the feared event. Some risk sources may be more likely to act than others. For example, if an unauthorized access to fitness data is made possible by exploitation of a functional error in the SMA then the likely risk sources are rogue hackers or rogue operators of the system or rogue UI administrators[29]. On the other hand, excessive collection of fitness data can occur just because the data controller (service provider) decides to do so. Thus, for each path in the harm tree, we consider only the most likely risk source.

Likelihoods can be computed in different ways, either symbolically (based on a fixed scale of levels such as “negligible”, “limited”, “significant”, etc.) or using numerical values (probabilities). Each approach has its benefits and drawbacks. Typically, probabilities may be difficult to estimate for input values and may look difficult to grasp by decision makers. In contrast, symbolic values are sometimes too fuzzy and may lead to different interpretations. We propose the use of a combined approach here, with symbolic input and output values which are converted into numerical values for processing based on the harm trees and converted back into symbolic values for the final output (likelihood of the

[29]The UMS administrator already has access to fitness data

harm). We provide an example of this approach in Section 4.2.2. We wish to emphasize however, that different choices of representation can be made by the analyst, provided that they are properly documented and justified.

The complete steps for computing likelihood are as follows:

1. Find the value of *exploitability* for each leaf node in the harm tree.
2. For each exploitation, choose the values of the relevant attributes of the risk source most likely to exploit the privacy weakness leading to the harm.
3. Find out the likelihood of each of these exploitations from the above *exploitability* value and values of the relevant risk source attributes.
4. Compute the likelihood of each feared event and harm according to the following rules[30], where P_i is the likelihood of ith child node:
   - R1. AND node with independent child nodes: $\prod_i P_i$.
   - R2. AND node with dependent child nodes[31]: $Min_i(P_i)$, i.e., minimum of the likelihoods of the child nodes.
   - R3. OR node with independent child nodes: $1 - \prod_i (1 - P_i)$.
   - R4. OR node with dependent child nodes[32]: $\sum_i P_i$.

4.2.2 Illustration: Risk level assessment for the FT System

We evaluate the risk levels for the three harms "undesirable disclosure of intimate personal habits to the public (H.1)", "undesirable disclosure of intimate personal habits to friends (H.3)" and "increased health insurance premium (H.2)" in Figure 7, Figure 8 and Figure 9. At the leaf nodes of the harm trees, we show (in curly braces) the exploitation likelihoods. Table 9 shows the how these likelihoods can be derived from the *exploitability* of the privacy weaknesses and the relevant attributes of the risk sources who perform the exploitation. At each AND or OR node, we show the rule (in curly braces) used for combining the likelihoods of the child nodes. Each nodes denoting a feared event is associated with the likelihood of the corresponding feared event and the root node is associated with the likelihood of the harm.

We use the following symbolic values for likelihood values (p):

1. *Negligible (N)* for $p < 0.01\%$;
2. *Limited (L)* for $0.01\% \leq p < 0.1\%$;
3. *Intermediate (I)* for $0.1\% \leq p < 1\%$;

[30] The rules are applied bottom-up.

[31] In order to err on the safe side in terms of privacy protection, we consider dependent nodes such that one node may imply another node.

[32] In order to err on the safe side in terms of privacy protection, we consider dependent nodes such that one node may exclude another node.

4. *Significant (S)* for $1\% \leq p < 10\%$;
5. *Maximum (M)* for $p \geq 10\%$.

Based on the input values (which are assumed to result from the expertise of the analyst) shown in Figure 7, Figure 8 and Figure 9 respectively, the risk levels of H.1, H.3 and H.2 are evaluated to *(significant, maximum)*, *(limited, maximum)* and *(maximum, limited)* respectively. At this stage, the decision maker (with the help of the analyst) can decide whether these risks are acceptable and, for the risks which are not deemed acceptable, choose appropriate counter-measures.

Since severity is an inherent measure of the damage caused by a harm, it cannot be reduced. The only factor that is in our control is the likelihood of harms which in turn depends on the likelihood of feared events and those of privacy weaknesses. A counter-measure can reduce the likelihood of one or more privacy weaknesses and thus reduces the likelihood of the harm that these privacy weaknesses lead to. Therefore, the most appropriate set of counter-measures is one that brings the risk level of all harms associated with the system below a given acceptable level and at the same time leads to minimal costs for implementation. This set of counter-measures can thus be obtained by solving a suitable optimization problem with appropriate constraints on the budget and the reduced level of likelihood. We note here that counter-measures can be of different types: technical, organizational and legal. The costs of implementing these counter-measures can also be of various types: operational cost, manpower cost, training cost etc.

Likelihood of exploitation	Exploitability of privacy weaknesses	Relevant risk source attributes
Negligible	Low	Majority do not favour
Limited		Majority favour
Intermediate		All Favour
Limited	Medium	Majority do not favour
Significant		Majority favour
Maximum		All favour
Intermediate	High	Majority do not favour
Maximum		Majority favour
Maximum		All favour

Table 9: Measurement rule for likelihood of exploitation

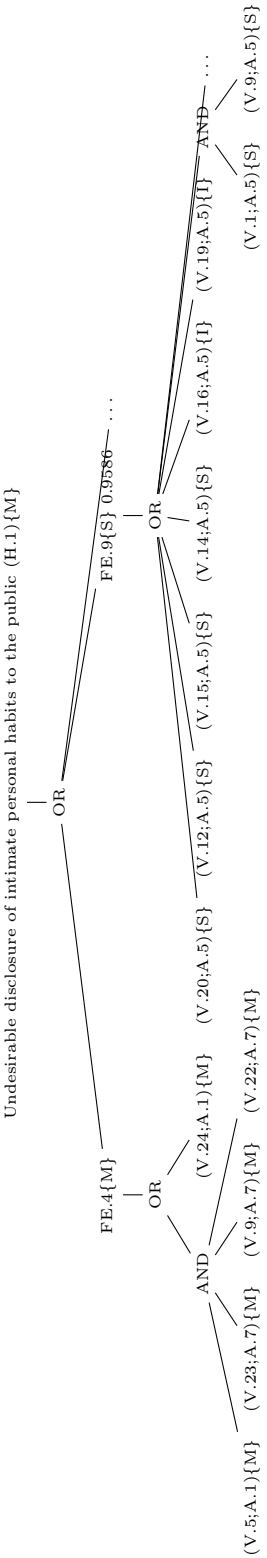


Figure 7: Risk level assessment for undesirable disclosure of intimate personal habits to the public (H.1)

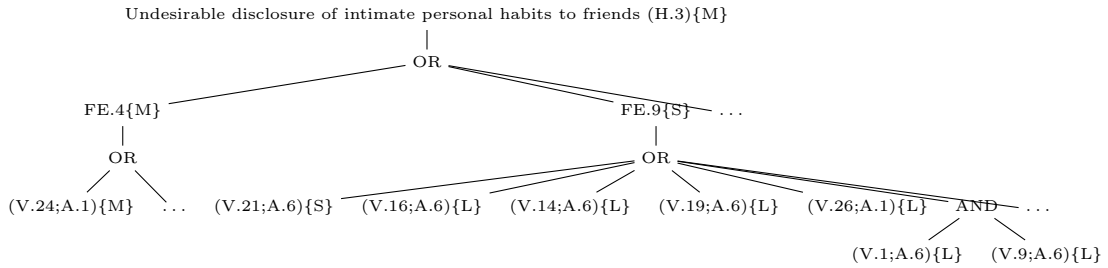


Figure 8: Risk level assessment for undesirable disclosure of intimate personal habits to friends (H.3)

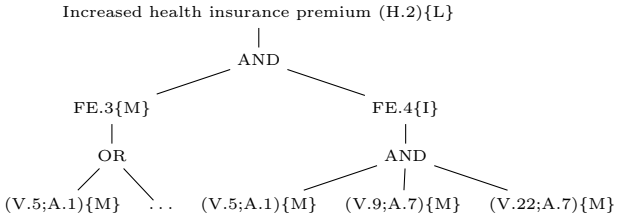


Figure 9: Risk level assessment for increased health insurance premium (H.2)

5 Related works

As discussed in the introduction, PRA should be embedded within a more general privacy impact assessment (PIA) as it corresponds to the technical part of a PIA. The literature on PIA mostly consists of: 1) proposals [50] focussing on organizational and management level tasks such as PIA team formation, preparation of a PIA plan, agreement on budget, etc. but only indicative about privacy risk analysis (PRA) steps; 2) proposals [11, 19, 20, 21, 22, 24, 31] focussing almost entirely PRA and 3) proposals [6, 8] that describe all steps of a PIA (including risk analysis) in some details. Since the focus of this work is solely PRA, we only discuss the PIA process described by Wright [50] and devote the the rest of this section to discuss how our work deviates from the second and third types of proposals.

The PIAF (Privacy Risk Assessment Framework) project has reviewed various existing PIA processes and methodologies [5, 32, 33, 34, 35, 36, 37] and has proposed an optimized PIA process [50]. When compared to the second and third types of proposals [6, 8, 11, 19, 20, 21, 22, 24, 31], the overall description of the PIA process [50] is at a higher level, focussing on what needs to be done rather than the precise details about how it is to be done. The PIAF framework defines the phases of a PIA that need to be carried out at the organizational and management levels such as PIA team formation, preparation of a PIA plan, agreement on a budget, identification and consultation with project stakeholders, third-party review and/or audit of the PIA, embedding privacy awareness in the organization and ensuring accountability, etc. It also includes more technically oriented steps such as the analysis of information flows and privacy impacts

and risk identification, but they are only indicative. For example, it is mentioned that risks should be assessed for their likelihood and consequences but there is no detailed description on how this assessment can be done. It does not go either into the details of system description, feared events or harms. Wright [50] stresses the importance of identifying all project stakeholders, i.e., whoever may be affected by the project, technology or service (such as regulatory authority, customers, citizen advocacy groups, service providers and manufacturers) so that they can be adequately consulted during the PIA process. He suggests that the range and number of stakeholders to be consulted should be a function of the privacy risks, assumptions about the frequency and consequences of these risks, and the number of consumers who can be impacted.

In the rest of this section, we discuss other PRA methodologies [6, 8, 11, 19, 20, 21, 22, 24, 31] and relate them to PRIAM in terms of terminology and methodology.

The literature on PRA methodologies use a variety of terminologies and definitions to refer to PRA components. Vulnerability [6, 8, 19, 20, 21, 24] is the most commonly used term for privacy weakness. It has also been referred to as "pre-condition" in [22, 52]. Some works [8, 19, 20, 21] contain no specific reference to privacy harms but refer to the impact of feared events on data subjects, termed "prejudicial effect", while measuring the severity of feared events. Others [6, 11, 31] also consider impacts for system operators or organizations. The term feared events has rarely been used in the sense of our definition. The CNIL methodology [19] refers to a feared event as an *"incident that affects availability, integrity or confidentiality of primary assets"*. The updated version of this methodology [21] re-defines it as *"breach of personal data security likely to have impacts on data subjects' privacy"*. The latter definition is the closest in the literature to what we mean by feared events in this work. No other work uses the term feared events. The LINDDUN framework [22, 52] discusses a number of privacy threats and also identifies events (privacy weaknesses in our terminology) that may lead to any of them. It does not define feared events. In [9], threats are not explicitly defined but it has been stated that threats lead to privacy harms. Threats, in their context, may arise from data processing: unjustifiable or excessive data collection, use or storage of inaccurate or outdated data, inappropriate use of data, lost or stolen data, unjustifiable or unauthorized access, transfer, sharing or publishing of data. Similarly, according to Oetzel and Spiekermann [31], threats prevent reaching a privacy target which represents what needs to be achieved for privacy protection, derived from EU privacy laws. The concept of privacy target is also used in the BSI framework [6]. In Friginal et al. [24], threat sources lead to threat events that affect privacy assets. They do not differentiate between threats and feared events and focus on one specific type of threat, the disclosure of assets. In some works [22, 24, 52], the terms "attacker" or "adversary" are used instead of risk sources. Unlike our definition, the CNIL guidelines [19, 20, 21] and the PIA on smart grids [8] use the term risk sources to refer to both human and non-human sources of risk. In this work, we have chosen the terminologies such that they carry as little security connotation as possible. Through them, we have tried to emphasize that the impact of privacy breaches is significantly different from that of security incidents and their causes may not always involve malicious actors or intentions.

In PRIAM, we show all the information required for the risk assessment process and indicate how they can be gathered by clearly identifying various attribute-attribute, attribute-category and category-category links. We also consider the influence of external factors such as social or legal norms as *norms* in determining certain categories and attributes. For example, we show that different attributes of data such as *form*, *retention*, *sensitivity*, *volume*, etc. along with attributes of other components such as the system can help to determine categories of privacy weaknesses and feared events. Such links are not well-established or, at least, not well-depicted in other works [8, 11, 20, 21, 22, 24, 31, 52]. The absence of such links raises questions about the completeness of the lists of data, feared events, privacy weaknesses, harms, risk sources, etc. considered in them. In our case, *victims* and *intensity* direct the measurement of severity of harms. In [6], only duration of the adverse impact is considered when assigning a value. Most works do not consider an exhaustive list of categories of harms. Some works consider only social standing, reputation, financial well-being, personal freedom [6,31] whereas others [20,21] consider physical, material and moral impacts. In some use cases, such as smart metering, social harms can play a significant role.

Risk assessment, in our work, entirely depends on harm trees which link privacy weaknesses and risk sources to harms, via feared events. The LINDDUN framework [22,52] uses threat trees to link what they define as threats to vulnerabilities in a system. Similarly, Friginal et al. [24] describe attack trees to link what they define as adverse impacts (e.g., disclosure of nearest friends of an user) to attack scenarios (e.g., hacking a device). However, these works do not provide an end-to-end link between privacy harms and privacy weaknesses. Harm trees clearly depict the contribution of different privacy weaknesses and risk sources in the occurrence of a particular harm.

We present the risk level of a harm as the pair: (severity, likelihood). Some proposals [11] include the computation of risk as a product of likelihood and impact. Others have used a risk map with severity and likelihood on its axes [8, 19, 20, 21] to plot estimated risks.

6 Conclusion

The PRIAM methodology, introduced in this report, makes it possible to conduct a PRA in a systematic and traceable way. In addition, it provides a set of components, attributes and categories which can be very helpful to reduce the risk of overlooking or under-estimating key factors for the evaluation of the privacy risks. Based on this analysis, it is possible to select a set of counter-measures that brings the risk level of all harms associated with the system below a given acceptable level and at the same time leads to minimal costs for implementation by solving a suitable optimization problem with appropriate constraints on the budget and the reduced level of likelihood. We leave detailed work on counter-measure selection based on PRIAM for future work. Harm trees illustrated in Section 4 can be the basis of selecting counter-measures that minimize risks for all harms and also satisfy a suitable budget. A study of all harm trees corresponding to harms whose risk levels are above a given acceptable threshold also reveal the privacy

weaknesses that have the strongest impact on these harms. For example, Figure 4, Figure 6 and Figure 5 reveal that weak anonymization of data is a common privacy weakness. So the analyst can decide which privacy weaknesses should be mitigated first.

Appendix A

Components	Categories	Attributes
Data	1. Identification data 2. Economic and financial information 3. Health information 4. Genetic information 5. Behavioral information 6. Technical data 7. Location data 8. Contact information 9. Information about professional life 10. Information about one's origin 11. Information about personal life 12. Judicial information 13. Information about personal belief	1. Related to nature of data (a) Sensitivity 2. Related to data format (a) Representation (b) Form (c) Precision (d) Volume 3. Related to context (a) Origin (b) Purpose (c) Retention 4. Related to control (a) Visibility (b) Intervenability
System	✗	1. Functional specification 2. Interface 3. Data flows 4. Supporting assets 5. Actors
Stakeholders	1. Data subject 2. Data controller 3. Data processor 4. Third parties	1. Relationships 2. Data flow view
Risk sources	1. Data subject 2. Data controller 3. Data processor 4. Third parties	1. Nature (a) Individual vs. organization (b) Insider vs. outsider 2. Level of motivation (a) Value (b) Motivation / fear 3. Resources (a) Background information (b) Access rights (c) Tools / skills, computation power

Components	**Categories**	**Attributes**
Privacy weaknesses	1. Weaknesses introduced by design choices or choices of functionalities 2. System design errors 3. Implementation errors	1. Exploitability
Feared events	1. Excessive data collection without consent 2. Unauthorized access to data 3. Unauthorized modification of data 4. Use of data for unauthorized purpose 5. Data inference including re-identification 6. Storage or use of inaccurate data 7. Disclosure to unauthorized actors, publication 8. Retaining data more than necessary, including lack of deletion or ineffective deletion	1. Scale 2. Irreversibility
Privacy harms	1. Physical harms 2. Economic or financial harms 3. Societal or architectural harms 4. Mental or psychological harms 5. Harms to dignity or reputation	1. Victims of harm (a) Individual (b) Society (c) Special groups 2. Intensity

Table 10: A summary of the categories and attributes of different components of PRIAM

Types of supporting assets	Examples
Hardware	One database server, application servers, load balancer, clients (PC, notebook, tablet, mobile phone, printer, etc.), storage media (semiconductor, optical, paper), network components (switch, router, bridge, gateway, firewall, modem), tracking devices, wireless sync dongle
Applications	FMA, UDMA, SMA, TA, TCA, SNA
Data stores	TDS, UDS
Software environment	standard software, operating systems, device driver, firmware, services (mail, file, etc.)

Table 11: Supporting Assets for the FT System

Types of controls	Examples
Technical measures	1) All user data are encrypted using AES-CCM during internal data storage and movement on the service provider's side; 2) TD authenticates with the TCS by computing a MAC over random bits, using a CBC-MAC with XTEA block cipher; 3) TCS and UMS communicate over an encrypted TLS connection.; 3) 128 bit keys are used. Keys are are renewed (old data re-keyed and new data encrypted with new key) once a year or whenever a compromise is suspected. TLS is used for securing keys in transit.; 4) Strong random number generators for generation of cryptographic parameters are used.; 5) Integrity and authenticity of data are verified before acting on them further.; 6) Users can modify privacy settings to make any information visible only to themselves or only to friends or to anyone. All data are public by default.; 7) Users can disable automatic sync and live data mode.; 8) Users can enable or disable at any time sharing of personally identifiable data with third party service providers such as social networking sites and health data storage providers.; 9) Detailed network device, operating system, web server, mail server, database server, application logging with built in tamper detection, storage in read-only media and access privilege restricted only to UMS administrators. Logs are reviewed periodically. Access to logs require prior approval and is recorded and monitored. Log data is not shared with any third party.; 10) Account lock-out period of 10 minutes when multiple log-in failure occurs.; 11) Passwords cannot be less than 8 characters. A secure password recovery system is also implemented. Passwords are transmitted over TLS.
Organizational measures	1) Disaster recovery program for critical business applications such as SMA, FMA and UDMA; 2) Establishment of dual role for key custodian so that the knowledges of two individuals are required to perform key management tasks.; 3) Frequent training and awareness programs for UMS administrators and operators enabling them to practice secure data handling.; 4) Employ trustworthy and trained UMS administrators to understand their responsibilities as custodians of cryptographic keys, reviewer of system logs, etc. They must sign a form stating that they understand their responsibilities.; 5) Information security policy and supporting standards and controls in which mandatory and recommended policy statements include, among others, access control, asset management, communications and operations security, human resources security, information systems acquisition, development and maintenance, physical and environmental security and risk assessment.; 6) Security certification process for applications and systems to confirm that they abide by the organization's information security policy and secure application development standards.; 7) Security incident management program to effectively control and remedy security related incidents.
Legal measures	1) Data handling policy for international users: subject to US laws, compliance with US-EU Safe Harbour Framework and US-Swiss Safe Harbour Framework with certification of adherence made available; 2) Policy for sharing data with third parties: de-identified data can be sold or used for different purposes such as research on health and fitness; identifiable data can be shared to fulfil legal obligations and in case of merger, bankruptcy, sale of assets, etc.; 3) The service is not meant for children below the age of 13 years; 4) Contract between the service provider and the third party handling Purchase Management system, with commitment to safeguard personal data received from the former.; 5) Privacy statement and disclaimers on User Interface for users to agree before opening an account. It specifies the following: i) types of data collected by the service provider; ii) the purpose of the collection for each type of data; iii) retention period of data; iv) policy for sharing data with third parties; v) policies for children; vi) how to modify data, deactivate accounts, etc. vii) data handling policy for international users.

Table 12: Controls implemented in the FT System

References

[1] Is Big Brother in your grocery cart? http://www.nocards.org. Accessed: 2016-02-15.

[2] EU directive 95/46/EC – The Data Protection Directive. https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm, 1995. Accessed: 2015-10-01.

[3] Privacy Impact Assessments. http://www.xamax.com.au/DV/PIA.html, 1998.

[4] Understanding risk through attack tree analysis. https://www.amenaza.com/downloads/docs/Methodology.pdf, 2004. Accessed: 2016-02-08.

[5] Privacy Impact Assessments - A Guide for the Victorian Public Sector. http://www.unimelb.edu.au/unisec/privacy/pdf/OVPC%20PIA%20Guide%202009.pdf, 2009. Accessed: 2015-10-01.

[6] Privacy Impact Assessment for RFID Applications. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy-Impact-Assessment-Guideline-Langfassung.pdf-blob=publicationFile, 2011. Accessed: 2015-09-25.

[7] Working Party 29 Opinion 08/2012 providing further input on the data protection reform discussions. http://idpc.gov.mt/dbfile.aspx/wp-199.pdf, 2012. Accessed: 2015-10-01.

[8] Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems. https://ec.europa.eu/energy/sites/ener/files/documents/2014-dpia-smart-grids-forces.pdf, 2014. Accessed: 2015-09-25.

[9] A Risk-based Approach to Privacy: Improving Effectiveness in Practice. https://www.hunton.com/files/upload/Post-Paris-Risk-Paper-June-2014.pdf, 2014. Accessed: 2015-10-01.

[10] Why Stop Smart Meters. http://stopsmartmeters.org/why-stop-smart-meters/, 2014. Accessed: 2016-01-02.

[11] Privacy Risk Management for Federal Information Systems. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir-8062-draft.pdf, 2015.

[12] Alessandra Bagnato, Barbara Kordy, Per Håkon Meland, and Patrick Schweitzer. Attribute decoration of attack–defense trees. *International Journal of Secure Software Engineering (IJSSE)*, 3(2):1–35, 2012.

[13] Felicity Baringer. New electricity meters stirs fear. http://www.nytimes.com/2011/01/31/science/earth/31meters.html, 2011. Accessed: 2016-01-02.

[14] Eric J Byres, Matthew Franz, and Darrin Miller. The use of attack trees in assessing vulnerabilities in SCADA systems. In *Proceedings of the international infrastructure survivability workshop*. Citeseer, 2004.

[15] Ryan Calo. Boundaries of Privacy Harm, The. *Ind. LJ*, 86:1131, 2011.

[16] Eric Clausing, Michael Schiefer, Ulf Lösche, and Maik Morgenstern. Security evaluation of nine fitness trackers. 2015.

[17] Julie E Cohen. Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, pages 1373–1438, 2000.

[18] Britt Cyr, Webb Horn, Daniela Miao, and Michael Specter. Security analysis of wearable fitness devices (fitbit). *Massachusetts Institute of Technology*, 2014.

[19] Commission Nationale de l'Informatique et des Libertes. Methodology for privacy Risk Management – How to Implement the Data Protection Act, 2012.

[20] Commission Nationale de l'Informatique et des Libertes. Methodology for Privacy Risk Management – How to Implement the Data Protection Act, 2015.

[21] Commission Nationale de l'Informatique et des Libertes. Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA), 2015.

[22] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. A privacy threat analysis framework: supporting the elicitation and fulfilment of privacy requirements. *Requirements Engineering*, 16(1):3–32, 2011.

[23] Emily Field. Biggest Privacy Problems in Fitness Trackers Still To Come. http://www.law360.com/articles/686145/biggest-privacy-problems-in-fitness-trackers-still-to-come, 2015.

[24] Jesús Friginal, Jérémie Guiochet, and Marc-Olivier Killijian. Towards a Privacy Risk Assessment Methodology for Location-Based Systems. In *Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 748–753. Springer, 2014.

[25] Eloise Gratton. Health-tracking bracelets and privacy issues. http://www.eloisegratton.com/blog/2014/12/20/health-tracking-bracelets-and-privacy-issues/, 2014.

[26] Kashmir Hill. Fitbit Moves Quickly After Users' Sex Stats Exposed. Forbes, 2011.

[27] Barbara Kordy, Piotr Kordy, Sjouke Mauw, and Patrick Schweitzer. Adtool: security analysis with attack–defense trees. In *Quantitative Evaluation of Systems*, pages 173–176. Springer, 2013.

[28] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Attack–defense trees. *Journal of Logic and Computation*, page exs029, 2012.

[29] Mikhail Lisovich, Deirdre K Mulligan, Stephen B Wicker, et al. Inferring personal information from demand-response systems. *Security & Privacy, IEEE*, 8(1):11–20, 2010.

[30] Teena Maddox. The dark side of wearables: How they're secretly jeopardizing your security and privacy. http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy 2015. Accessed: 2016-02-15.

[31] Marie Caroline Oetzel and Sarah Spiekermann. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, 23(2):126–150, 2014.

[32] Office of Management and Budget. OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. https://www.whitehouse.gov/omb/memoranda-m03-22, 2003. Accessed: 2015-09-23.

[33] Office of the Chief Information and Privacy Officer. Privacy Impact Assessment Guide for the Ontario Public Service. Toronto: Queen's Printer for Ontario, 2010.

[34] Office of the Information Privacy Commissioner of Alberta. Privacy Impact Assessment (PIA) Requirements, 2009.

[35] Office of the Privacy Commissioner. Privacy Impact Assessment Handbook. https://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf, 2007. Accessed: 2015-10-01.

[36] Office of the Privacy Commissioner. Privacy Impact Assessment Guide. http://www.oaic.gov.au/privacy/privacy-archive/privacy-resources-archive/privacy-impact-assessment-guide, 2010. Accessed: 2015-10-01.

[37] Information Commissioner's Office. Privacy Impact Assessment Handbook, Version 2.0. Cheshire, UK: Wilmslow. www.adls.ac.uk/wp-content/uploads/2011/08/PIA-handbook.pdf, 2003. Accessed: 2015-09-23.

[38] Igor Oskolkov. Your fitness is their business. Nothing personal. https://blog.kaspersky.com/fitness-trackers-privacy/6480/, 2014. Accessed: 2016-02-12.

[39] European Parliament. General Data Protection Regulation, 2014.

[40] Scott R Peppet. Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93:85, 2014.

[41] Wolter Pieters and Mohsen Davarynejad. Calculating adversarial risk from attack trees: Control strength and probabilistic attackers. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pages 201–215. Springer, 2015.

[42] Mosaddequr Rahman, Bogdan Carbunar, and Umut Topkara. SensCrypt: A Secure Protocol for Managing Low Power Fitness Trackers. In *Network Protocols (ICNP), 2014 IEEE 22nd International Conference on*, pages 191–196. IEEE, 2014.

[43] Indrajit Ray and Nayot Poolsapassit. Using attack trees to identify malicious attacks from authorized insiders. In *Computer Security–ESORICS 2005*, pages 231–246. Springer, 2005.

[44] Arpan Roy, Dong Seong Kim, and Kishor S Trivedi. Cyber security analysis using attack countermeasure trees. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, page 28. ACM, 2010.

[45] Arpan Roy, Dong Seong Kim, and Kishor S Trivedi. Attack countermeasure trees (act): towards unifying the constructs of attack and defense trees. *Security and Communication Networks*, 5(8):929–943, 2012.

[46] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

[47] Paul M Schwartz. Privacy and democracy in cyberspace. *Vand. L. Rev.*, 52:1607, 1999.

[48] Paul M Schwartz and Daniel J Solove. PII Problem: Privacy and a New Concept of Personally Identifiable Information, The. *NYUL Rev.*, 86:1814, 2011.

[49] Daniel J Solove. A taxonomy of privacy. *University of Pennsylvania law review*, pages 477–564, 2006.

[50] David Wright. Making privacy impact assessment more effective. *The Information Society*, 29(5):307–315, 2013.

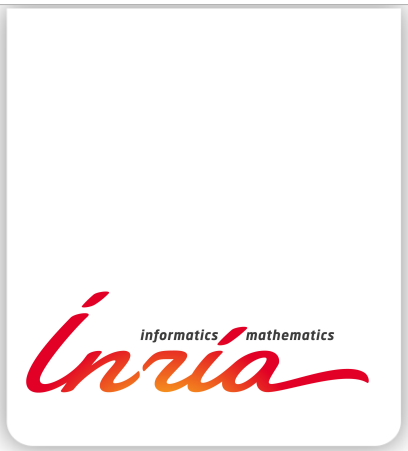
[51] David Wright, Rachel Finn, and Rowena Rodrigues. A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research*, 9(1), 2013.

[52] Kim Wuyts. Privacy Threats in Software Architectures. *status: accepted*, 2014.

[53] Ronald R Yager. OWA trees and their role in security modeling using attack trees. *Information Sciences*, 176(20):2933–2959, 2006.

[54] Wei Zhou and Selwyn Piramuthu. Security/privacy of wearable fitness tracking iot devices. In *Information Systems and Technologies (CISTI), 2014 9th Iberian Conference on*, pages 1–5. IEEE, 2014.

[55] Harald Zwingelberg and Marit Hansen. Privacy Protection Goals and their implications for eID systems. In *Privacy and Identity Management for Life*, pages 245–260. Springer, 2012.



RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée

655 avenue de l'Europe Montbonnot

38334 Saint Ismier Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399