Institutional Violence Complaints in Argentina: A Privacy Study

Jorge Roa[1], Pablo Villarreal[1], Marcelo Fantinato[2]
Patrick C. K. Hung[3,4], Laura Rafferty[3]
[1]*CIDISI-UTN-CONICET, Santa Fe, Argentina*
[2]*School of Arts, Sciences and Humanities, University of São Paulo, Brazil*
[3]*Faculty of Business and IT, University of Ontario Institute of Technology, Canada*
[4] *Department of Electronic Engineering, National Taipei University of Technology, Taiwan*
{jroa, pvillarr}@frsf.utn.edu.ar; m.fantinato@usp.br
{patrick.hung, laura.rafferty}@uoit.ca

Abstract

Argentina is a federal republic located in South America. Despite Argentina's redemocratization in 1983, conditions favoring human rights abuses still persist. Institutional violence refers to structured practices of human rights violation by state officials belonging to public institutions. In this paper, we outline and discuss privacy issues in institutional violence complaints in Argentina. To this aim, we defined a BPMN process model for registering victims' complaints in a database, and proposed an approach to investigate the privacy of such process from a threat modeling perspective. With the approach, we identified privacy threats of information disclosure and content unawareness, and defined privacy requirements and controls needed to mitigate these threats.

1. Introduction

Argentina is a federal republic member of the G-20 world's largest economies and is second in size and third in population in South America. It is a federation of twenty-three provinces and one autonomous city, Buenos Aires. Provinces hold all the power they chose not to delegate to the federal government. They must be representative republics in compliance with the Federal Constitution.

Despite Argentina's redemocratization in 1983, conditions favoring human rights abuses still persist [1]. Specific human rights abuses (e.g., torture, disappearances, and murder) that resemble practices common under dictatorship's state terrorism (1976 to 1983) continue to take place [1]. The law prohibits torture and other cruel, inhuman, or degrading treatment or punishment and provides penalties for it.

In 2012, the National Registry of Cases of Torture and/or Maltreatment (NRCT) attempted to comply with international human right treatments. The NRCT encourages the operational implementation of the optional protocol to the convention against torture and other cruel, inhuman or degrading treatment or punishment [8]. For this, concrete cases of violation of rights and torture are registered through regular visits to confinement places, and by spontaneous communications of victims and their relatives to the Office of Procurator and Commissioner.

As a result, the Criminal Court of Cassation's Office in Buenos Aires reported that there were 265 complaints of torture and mistreatment by law enforcement officers during arrest or institutional confinement from January to April 2015. On the other hand, the Office of Public Defenders in the province of Santa Fe reported 180 complaints from December 2014 to September 2015 [2].

Institutional violence refers to structured practices of human rights violation by state officials belonging to public institutions such as security forces, armed forces, prison services and health effectors in contexts of restriction of autonomy and/or liberty, e.g., arrests, imprisonments, custodies, cares, hospitalizations, etc. Since complaints may individualize abusers (e.g., police officers), some victims express reluctance to make judicial complaints because of their fear of physical, mental and access rights reprisals adopted by state officials after each complaint.

In this context, protecting privacy of victims' complaints is an imperative concern. Hung and Cheng [4] define information privacy as "an individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization." Privacy rules can be achieved through privacy preserving mechanisms such as encryption and access control. In this work, we outline and discuss privacy issues in institutional

URI: http://hdl.handle.net/10125/41648
ISBN: 978-0-9981331-0-2

violence complaints in Argentina. To this aim, we defined a BPMN (Business Process Model and Notation) [19] process model for registering victims' complaints in a database, and proposed an approach to investigate the privacy of such process from a threat modeling perspective. The approach was adapted from Microsoft's Threat Modeling Principles [12] and STRIDE Model [13], and the LINDDUN methodology [17]. By applying the approach, we identified privacy threats and defined privacy requirements and controls needed to mitigate these threats.

This paper is organized as follows. Section 2 provides a literature review. Section 3 presents the procedure for surveying institutional violence complaints in Argentina. Section 4 presents privacy threat assessment. Section 5 provides a study on privacy threats. Section 6 concludes the paper and presents future work.

2. Related work

There are a number of related research works in this area. For example, Debnath et al. [15] conceptually designed the IT support for human rights watching, police transparency and police performance evaluation in the province of Chubut, Argentina. To this aim, they proposed a web application, which tracks and records Police Station activities and provide citizens the opportunity to evaluate Police performance, and hence it can be used as human rights watching tool.

Van den Braak et al. [14] proposed a framework to support secure data integration and sharing for interorganizational collaboration in the public sector. It requires a trusted third party that manages access control to personal information and helps protect the privacy of parties. This framework could be useful for the exchange of data between the NRCT and other public organizations or NGOs, but for the tasks of data collection and registration of cases of torture, it is necessary to include other security and privacy methods from the inside. Van Veenstra et al. [25] found that the main threats to information security and privacy in several public organizations in the Netherlands came from the inside. For instance, "employees of organizations sometimes accessed information that they did not need in order to perform their tasks, such as information concerning celebrities".

Zuiderwijk et al. [10] presented guidelines for identifying issues for opening up governmental judicial research data. Guidelines were determined by investigating the publishing processes at the Dutch Research and Documentation Centre. They determined the following issues that should be taken into account when opening up a dataset: confidentiality, deletion policies, embargo placement, cost and time consumption, ownership, privacy-sensitivity and anonymization, lack of metadata, reuse of data by the organization itself, policy-sensitivity and unlawfulness. These guidelines could be useful to minimize information disclosure of complaints in the NRCT.

Van den Braak et al. [9] described how judicial data can be collected, combined, and analyzed such that the privacy of individuals in society is not violated. They explained what safety measures have to be taken in the process of data integration process to better respect privacy laws and regulations, and hence minimize the risk of exposing the identity of individuals.

Parks et al. [20] outline consequences of privacy safeguard in the healthcare domain. They focus on how privacy-preserving techniques establish a trade-off between meeting privacy requirements and the execution of healthcare processes. These consequences should be carefully considered when proposing privacy-preserving techniques for the process of registering institutional violence complaints.

Koops and Leenes [21] discuss practical implications of "privacy by design" and the complexity of encoding data protection requirements in software. This is because of privacy must co-exist with other requirements like security, functionality, operational efficiency, organizational control, business processes, and usability. The authors conclude that "privacy by design should be approached less from a 'code' perspective, but rather from the perspective of 'communication' strategies". In this regard, there are privacy design strategies like the proposed by Deng et al. [17], Hoepman [22], Heurix et al. [23], or Hansen et al. [24] that consider privacy and data protection principles from the beginning of the development process.

The use of workflow management systems (WfMSs) could be a benefit for privacy strategies, since they could be applied on conceptual process models rather than software code, but they entail other challenges. In this regards, in [5] authors showed weaknesses of WfMSs to capture and enforce privacy policies such as conflict of interest, hiding personal data, or generalizing data, and provide extensions to the YAWL WfMS to cope with such issues. Similarly, Mülle et al. [6] and Ciuciu et. al. [3] propose structured text annotations in BPMN models to define privacy and security aspects related to users. However, none of these works explicitly mentions how to identify the privacy issues to be modeled.

In summary, none of these works has discussed privacy issues of institutional violence complaints. Existing work in the public sector focuses on data integration between different organizations, rather than on how to identify privacy issues from the inside. On the other hand, there are extensions to business process languages to cope with privacy specifications, but there is no approach to identify privacy threats from the beginning in process models. In this work, we propose an approach taking advantage of BPMN for registering institutional violence complaints.

3. Procedure for surveying institutional violence complaints in Argentina

The Optional Protocol to the United Nation (UN) Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment (OPCAT) establishes a procedure for visits to all places where persons are deprived of their liberty by independent international and national monitoring bodies [8]. Argentina was the first State in Latin America to ratify the OPCAT in 2004. The law for a national system of prevention was issued in April 2014 and the selection process of the members of the National Committee to Prevent Torture is still pending[1].

Besides NRCT, six provinces (Chaco, Mendoza, Misiones, Río Negro, Salta, and Tucumán) have adopted laws to create local preventive mechanisms to implement OPCAT, while others (Santa Fe, Neuquén, Corrientes, Córdoba, San Luis, Tierra del Fuego, and Buenos Aires) are in the process of debating such laws. The Santa Fe province created the Provincial Registry of Cases of Torture, Cruel, Inhuman and/or Degrading Abuse Police and other affectations Bad Practices and Human Rights within the scope of the Provincial Public Defense Service (SPPDP).

Figure 1 shows the procedure for collecting and receiving institutional violence complaints in Argentina. This procedure refers to public and open access documents such as laws, resolutions, and reports of the NRCT and the SPPDP registry. We use the term *registry* to refer to the database that contains information about institutional violence complaints in the context of the NRCT or the SPPDP registry. There are five general use cases for surveying and reporting situations of torture in public institutions.

Referring to the first use case, interviewers visit institutions where there are people deprived of liberty such as prisons, reformatories, or hospitals. In those places, victims are interviewed and fill up the forms to report new cases of tortures. Forms are sent to the database administrator. People deprived of liberty could be in hospitals when they are recovering from a disease or if they are under psychiatric treatment. In the second use case, complaints of tortures are received from witnesses or victims. These complaints are also registered in forms. Then, the forms are sent to the database administrator. In the third and fourth use cases, complaints are gathered from information published on newspapers or from NGOs and other organizations. For all of these cases, the database administrator registers all of their forms into the registry. Referring to the fifth use case, the database administrator generates statistical reports for their superior to be published to the public on the internet.

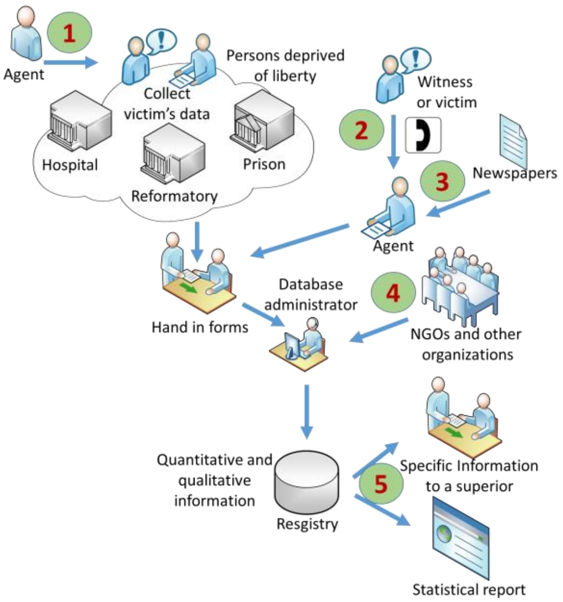


Figure 1. Use cases for surveying and reporting situations of torture

The form for surveying new cases of institutional violence was designed to be applied during inspections to places of penitentiary detention and youth custody. It is also meant to reconstruct information from communications by other institutional channels and surveys conducted by other organizations. As for the surveys, the interviewer proceeds to complete a form for each victim that connects one or more acts of torture and/or ill-treatment suffered in the span of the last 60 days at the time of the interview. It is assumed that paper forms are archived and secure.

A technical team edits the information recorded in confinement places to make it consistent. Then, information is entered into the registry as shown in Figure 1. Subsequently new analyses are performed to process the data statistically and qualitatively for preparing annual reports or partial reports.

According to Figure 1, the registry stores cases of abuse and/or torture prosecuted, but also cases reported to state agencies, human rights or NGOs. In addition to the most widespread modalities, such as physical aggressions, the registry considers different types of ill-treatments and tortures.

[1] http://www.apt.ch/en/opcat_pages/opcat-situation-84/?pdf=info_country

In the surveys, the form for each victim of acts of torture or ill-treatment (Figure 2) includes data about the receiving source, the victim and the facts, from a written summary and a series of closed and open fields to be completed by the interviewer. The information of the form is stored in the registry as shown in Figure 1.

4. Privacy threat assessment

In this section, we propose an approach to investigate the privacy of the procedure presented in Section 3 from a threat modeling perspective.

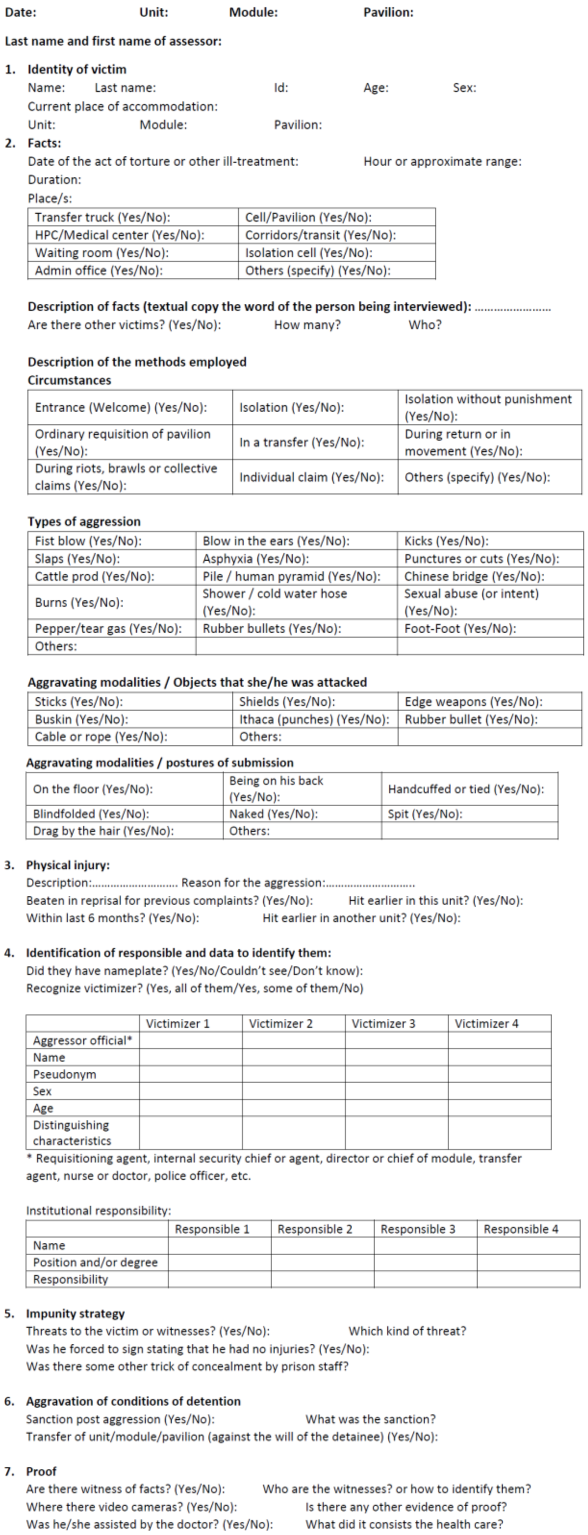
When it comes to any information technology, privacy and security are at the core of ensuring that goals are achieved effectively and without compromise of personal data. The three concerns of security are confidentiality, integrity and availability. Confidentiality means that access to information is restricted only to intended parties. Integrity means that data is accurate and consistent and has not been tampered with, while availability means that resources and data remain available when needed by the legitimate parties.

A security background is required for privacy. In particular, personally identifiable information is any type of information that can be linked to an individual, including their activities, preferences, history, conversations, etc. Information privacy goals can be achieved through privacy preserving mechanisms such as access control, privacy policies, and privacy preferences.

Privacy policies describe an organization's data practices. This includes a description of what information is collected from users, what the information is used for, how long it needs to be held, if and how the information should be shared to third parties, how long information needs to be retained, etc.

The user gives consent either implicitly or explicitly. Often, consent is implied just by using the services. Explicit consent can be given if the user is required to click "I agree" in regards to the privacy policy terms and conditions to receive services.

Threat modeling is a useful tool to assess risk associated with a system and provides a structured approach to security and privacy. Several approaches have been developed for threat modeling, one of the most widely adapted being Microsoft's Threat Modeling Process [12] and STRIDE model [13] for identifying six categories of security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This model presents a systematic approach to understanding and decomposing an application to identify security threats, however there is little focus on privacy.



Date: **Unit:** **Module:** **Pavilion:**

Last name and first name of assessor:

1. **Identity of victim**
   Name: Last name: Id: Age: Sex:
   Current place of accommodation:
   Unit: Module: Pavilion:
2. **Facts:**
   Date of the act of torture or other ill-treatment: Hour or approximate range:
   Duration:
   Place/s:

Transfer truck (Yes/No):	Cell/Pavilion (Yes/No):
HPC/Medical center (Yes/No):	Corridors/transit (Yes/No):
Waiting room (Yes/No):	Isolation cell (Yes/No):
Admin office (Yes/No):	Others (specify) (Yes/No):

Description of facts (textual copy the word of the person being interviewed): ....
Are there other victims? (Yes/No): How many? Who?

Description of the methods employed
Circumstances

Entrance (Welcome) (Yes/No):	Isolation (Yes/No):	Isolation without punishment (Yes/No):
Ordinary requisition of pavilion (Yes/No):	In a transfer (Yes/No):	During return or in movement (Yes/No):
During riots, brawls or collective claims (Yes/No):	Individual claim (Yes/No):	Others (specify) (Yes/No):

Types of aggression

Fist blow (Yes/No):	Blow in the ears (Yes/No):	Kicks (Yes/No):
Slaps (Yes/No):	Asphyxia (Yes/No):	Punctures or cuts (Yes/No):
Cattle prod (Yes/No):	Pile / human pyramid (Yes/No):	Chinese bridge (Yes/No):
Burns (Yes/No):	Shower / cold water hose (Yes/No):	Sexual abuse (or intent) (Yes/No):
Pepper/tear gas (Yes/No):	Rubber bullets (Yes/No):	Foot-Foot (Yes/No):
Others:		

Aggravating modalities / Objects that she/he was attacked

Sticks (Yes/No):	Shields (Yes/No):	Edge weapons (Yes/No):
Buskin (Yes/No):	Ithaca (punches) (Yes/No):	Rubber bullet (Yes/No):
Cable or rope (Yes/No):	Others:	

Aggravating modalities / postures of submission

On the floor (Yes/No):	Being on his back (Yes/No):	Handcuffed or tied (Yes/No):
Blindfolded (Yes/No):	Naked (Yes/No):	Spit (Yes/No):
Drag by the hair (Yes/No):	Others:	

3. **Physical injury:**
   Description:............................ Reason for the aggression:.............................
   Beaten in reprisal for previous complaints? (Yes/No): Hit earlier in this unit? (Yes/No):
   Within last 6 months? (Yes/No): Hit earlier in another unit? (Yes/No):

4. **Identification of responsible and data to identify them:**
   Did they have nameplate? (Yes/No/Couldn't see/Don't know):
   Recognize victimizer? (Yes, all of them/Yes, some of them/No)

	Victimizer 1	Victimizer 2	Victimizer 3	Victimizer 4
Aggressor official*				
Name				
Pseudonym				
Sex				
Age				
Distinguishing characteristics				

* Requisitioning agent, internal security chief or agent, director or chief of module, transfer agent, nurse or doctor, police officer, etc.

Institutional responsibility:

	Responsible 1	Responsible 2	Responsible 3	Responsible 4
Name				
Position and/or degree				
Responsibility				

5. **Impunity strategy**
   Threats to the victim or witnesses? (Yes/No): Which kind of threat?
   Was he forced to sign stating that he had no injuries? (Yes/No):
   Was there some other trick of concealment by prison staff?

6. **Aggravation of conditions of detention**
   Sanction post aggression (Yes/No): What was the sanction?
   Transfer of unit/module/pavilion (against the will of the detainee) (Yes/No):

7. **Proof**
   Are there witness of facts? (Yes/No): Who are the witnesses? or how to identify them?
   Where there video cameras? (Yes/No): Is there any other evidence of proof?
   Was he/she assisted by the doctor? (Yes/No): What did it consists the health care?

Figure 2. The form (translated from Spanish)

To preserve privacy, there must be a foundation of security. To achieve this, one must ensure that the system, for example in this context, the registry in

Figure 1, has a reasonable level of security mechanisms in place, and that personal information is protected from a security perspective.

Deng et al. [17] have developed a methodology called LINDDUN that provides a comprehensive privacy threat modeling framework. Like the STRIDE model, LINDDUN identifies privacy threats by using similar threat modeling principles (data flow diagrams, threat trees and trust boundaries) and mapping them to privacy properties based on the terminology defined by Pfitzmann et al. [18]. Misuse case scenarios and privacy threat tree patterns illustrate privacy attack scenarios, which are then prioritized through risk assessment techniques. In the final two steps of this methodology, mapping the privacy threats to privacy requirements allows for the identification of privacy enhancing solutions.

The following privacy threats are the basis of the LINDDUN methodology: (1) *linkability*, an attacker is able to distinguish whether two or more items of interest (e.g. subjects, messages, actions, etc.) are related or not within the system; (2) *identifiability*, an attacker can sufficiently identify a subject associated to an item of interest, such as the sender of a message; (3) *non-repudiation*, this allows an attacker to gather evidence to counter the claims of the repudiating party and to prove that a user knows, has done or has said something; (4) *detectability*, an attacker can distinguish whether an item exists or not, e.g. messages are sufficiently discernible from random noise; (5) *information disclosure*, personal information is exposed to individuals who are not supposed to have access to it; (6) *content unawareness*, a user is unaware of the information disclosed to the system; (7) *policy and consent noncompliance*, this means that even though the system shows its privacy policies to its users, there is no guarantee that the system actually complies to the advertised policies.

The above threats can be categorized into hard or soft privacy threats [17]. Our focus for this paper is on soft privacy: information disclosure and content awareness. Soft privacy is based on the assumption that the data subject is not in control of personal data, and must trust the data controllers (service providers). This is the domain of policies, access control and audit. In this model, the data subject provides personal data and the data controller is responsible for it. Policy consent and noncompliance is beyond the scope of this paper, which assumes that the system (i.e., the registry in Figure 1) complies with its privacy policies.

Based on the above threat modeling techniques, we have adapted our own technique appropriate for modeling privacy threats in this environment. Below is the threat modeling process we cover in the following sections, adapted from Microsoft's Threat Modeling Principles [12] and STRIDE Model [13], and the LINDDUN methodology [17]. We believe that this would provide an effective analysis of privacy threats in this procedure. Our approach, illustrated in Figure 3, uses a similar process as the three models discussed above, with the largest motivation from LINDDUN. Starting with an overview of the technical architecture, we identify personal data assets and data flow. Next, we use the LINDDUN methodology to identify privacy threats and threat agents, and illustrate methods of attack through threat trees.

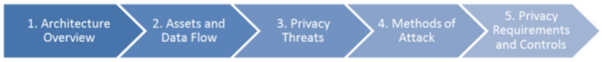


Figure 3. Threat modeling process

5. Privacy threats in institutional violence complaints

In this section, we analyze the law related to privacy in institutional violence complaints in Argentina, apply the proposed approach, and establish a discussion in this context.

The law related to institutional violence complaints consider some aspects related to privacy. However, it is not sufficient to protect the privacy of individuals. Law 26.827, Article 45 states that the consent of the victim to publish their data and personal information in reports, media or other ways of making the information public is always required [7]. However, the victim may not be aware of the consequences of making their data public. In this regards, the resolution N° 5 of the SPPDP[2] (2012, Annex I. 13) states that the interviewer should draw the attention of the victim providing information about the privacy policy of the Provincial Registry, where he can choose "preserving the identity of the complainant". However, this depends on the interviewer and the resolution does not guarantee identity preservation.

Law 26.827, Article 47 has to do with preserving the identity of victims, and state that disclosure of information could place the victim at risk [7]. Related to this law, the resolution N° 5 of the SPPDP (2012, Annex I. 16) states that any person who is somehow involved in the process of collection, referral, registration and publication of data shall maintain absolute confidentiality in relation to victims and preserve all data coming to their knowledge. However, these are rather warnings that are not enough to preserve identity of victims.

[2] SPPDP. Resolution 0005. 2012. http://www.sppdp.gob.ar/site/normativa/resoluciones/indice/2012/archivo/Resolucion-0005P-2012.pdf

Finally, the resolution N° 5 of the SPPDP (2012, Annex I. 19) states that the Deputy Secretary of the Provincial Registry shall arbitrate the means to take the necessary precautions to make safety records to ensure the proper safeguarding of data loaded into the Provincial Registry (e.g., backup, compressing, etc.). However, Secretary may not be aware of the precautions necessary to safeguard victim's data.

5.1 Identify privacy threats

From a policy perspective, any data sharing practices that may result in any of the LINDDUN threats discussed in Section 4 should be identified in the system's privacy policy. This work depends heavily on the assumption that the registry or the procedure has published an accurate privacy policy and also complies with it.

For the purpose of this paper, we address the threats of information disclosure and content unawareness. Information disclosure occurs when a user's personal information is exposed to individuals who are not supposed to have access to it. We assume that although information disclosure practices are outlined in the privacy policy, and the user has provided their consent, the user is not actually aware since they do not read or understand the policy. Content unawareness occurs when the user is unaware of the information that is collected on them, such as their personal information.

The Internet Engineering Task Force (IETF) RFC6973 on Privacy Considerations [16] provides more specific secondary threats that fall under the categories of information disclosure and content unawareness. In the proposed model, we attempt to prevent the following four categories of threats to victims:

- **Surveillance**: the observation or monitoring of an individual's communications or activities. The effects of surveillance on the individual can range from anxiety and discomfort to behavioral changes such as inhibition and self-censorship, and even to the perpetration of violence against the individual. The individual need not be aware of the surveillance so that it impacts their privacy – the possibility of surveillance may be enough to harm individual autonomy.
- **Secondary use**: the use of collected information about an individual without the individual's consent for a purpose different from that for which the information was collected. Secondary use may violate people's expectations or desires. The potential for secondary use can generate uncertainty on how one's information is used in the future, potentially discouraging information exchange in the first time.

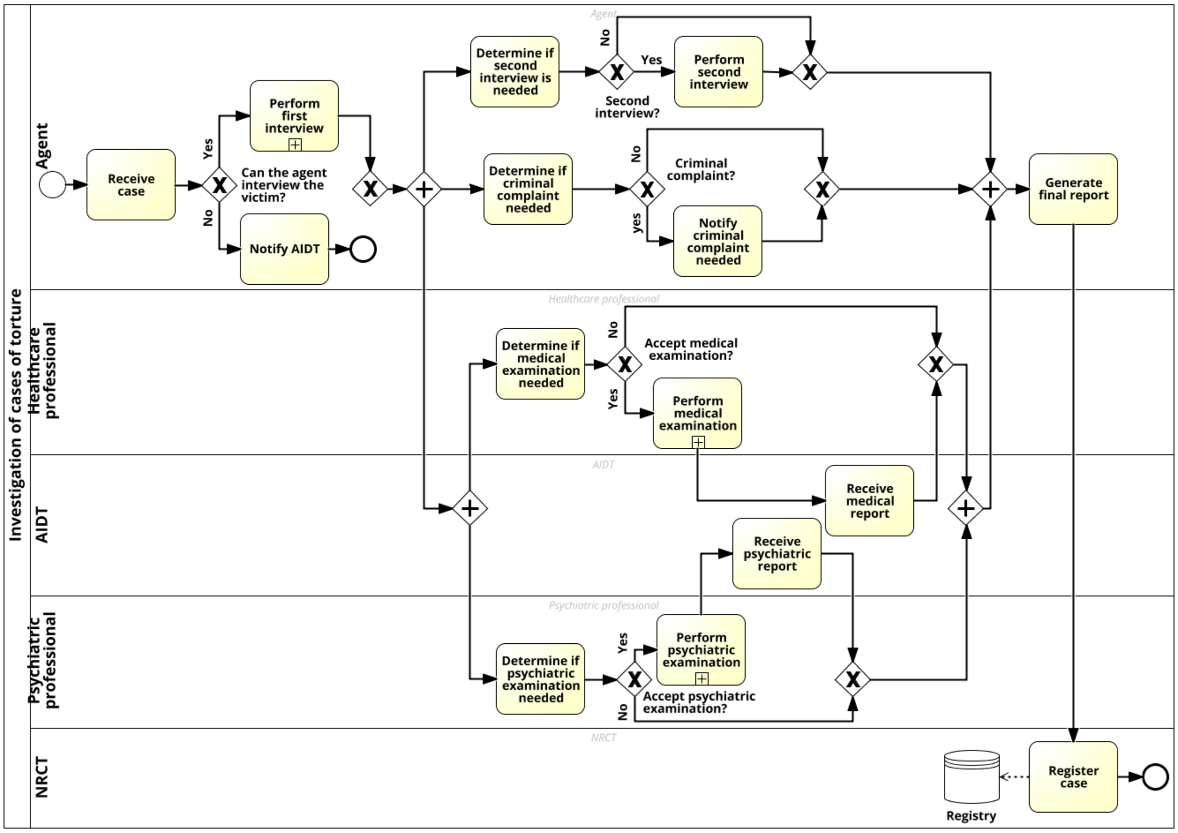

Investigation of cases of torture
Agent
Healthcare professional
AIDT
Psychiatric professional
NRCT
Agent
Receive case
Yes
No
Can the agent interview the victim?
Perform first interview
Notify AIDT
Determine if second interview is needed
No
Yes
Second interview?
Perform second interview
Determine if criminal complaint needed
No
Criminal complaint?
yes
Notify criminal complaint needed
Generate final report
Healthcare professional
Determine if medical examination needed
No
Accept medical examination?
Yes
Perform medical examination
AIDT
Receive medical report
Receive psychiatric report
Psychiatric professional
Determine if psychiatric examination needed
Yes
Perform psychiatric examination
No
Accept psychiatric examination?
NRCT
Registry
Register case

Figure 4. Procedure for surveying institutional violence complaints in BPMN

- **Disclosure**: the revelation of information about an individual that affects the way others judge this individual. Disclosure can violate individuals' expectations of the confidentiality of the data they share. The threat of disclosure may deter people from engaging in certain activities for fear of reputational harm, or simply because they do not wish to be observed.
- **Exclusion:** the failure to allow individuals to know about data that others have about them and to participate in its handling and use. Exclusion reduces accountability on of entities that maintain information about people and creates a sense of vulnerability in relation to individuals' ability to control how information about them is collected and used.

5.2 Mapping privacy threats to Data Flow Diagrams

Figure 4 shows the process for investigation of torture cases by means of a BPMN model. This model corresponds to use case 1 for collecting victim's data described in Figure 1. The process starts when an agent receives a case. If the agent cannot interview the victim, they must notify the AIDT (Area of investigation and documentation of cases of torture) and the process ends. Otherwise, the agent interviews the victim. After that, if a second interview is needed, the agent performs the interview. In parallel, the agent notifies whether a criminal complaint is needed. Additionally, a healthcare professional performs a medical examination in case it is needed, and then sends the report to the AIDT. Analogously, a psychiatric professional performs an examination and then sends the report to the AIDT. Once these activities are finished, the agent generates a report, the NRCT includes the case in the registry, and the process ends.

Table 1. Mapping BPMN to DFD elements

Entity	**User**
Process	Investigation of cases of torture
Data Store	Registry
Data Flow	- User data stream (victim to form) - Service data stream (form to agent) - Registry data stream (agent to database)

Since the privacy threat analysis of LINDDUN makes use of Data Flow Diagrams (DFDs) [17], based on this process model, Table 1 maps the BPMN model elements to DFD elements, whereas Table 2 maps the LINDDUN privacy threats to DFD element types (E: Entity, DF: data flow, DS: data store, P: process).

The threat of information disclosure occurs at the process, data store and data flow levels. This falls into the control of the registry, which outlines information disclosure practices in their privacy policy. While we assume that the registry has accurate policies as well as complies with them, the threat we are concerned with is related to the entity who agrees to disclose the information.

Content unawareness is a threat to the entity (user). The user is required to provide the necessary consent to process personal data. The goal of our model is to address the threats of content unawareness from the perspective of the user, putting them in control of information disclosure. This model addresses information disclosure from the entity's perspective who complies with information disclosure practices. This model is acting under the assumption that all the process, data store and data flow elements act in compliance with their policies and the consent of the victim.

Table 2. Mapping privacy threats to DFD elements

Threat Categories	**Entity**	**Process**	**Data Store**	**Data Flow**
Linkability	N/A	N/A	N/A	N/A
Identifiability	N/A	N/A	N/A	N/A
Non-repudiation		N/A	N/A	N/A
Detectability		N/A	N/A	N/A
Information **D**isclosure	T	A	A	A
Content **U**nawareness	T			
Policy/Consent **N**oncompliance		A	A	A

Legend: N/A=Not Applicable (Out of scope), T=Threats addressed, A=Assumed to Comply

5.3 Methods of attack

In this section, we observe the different methods an adversary can use to reach the data. First, we examine privacy threats based on Table 2 in order to determine privacy threat trees. Next, we create misuse case scenarios based on the threat tree patterns and propose privacy requirements and controls to mitigate these threats.

5.3.1 Privacy threat tree for information disclosure

Figure 5 refers to the privacy threat tree for information disclosure. For the purpose of this work, we are referring to intentional information disclosure, which is predefined by the registry and outlined in the privacy policy, rather than information disclosure as a result of security exploits. Personal information may be disclosed to other users or to a third party. The threats related to sharing a victim's personal data can lead to undesirable inferences of the victim's behavior and personal life. A victim's personal data sent to a third party can be used for customer profiling of the victim. Sharing personal data with other users puts the physical safety of the victim at risk if it is shared with an untrusted entity. For these reasons, a victim may choose not to consent to sharing their personal data depending on privacy policy practices.

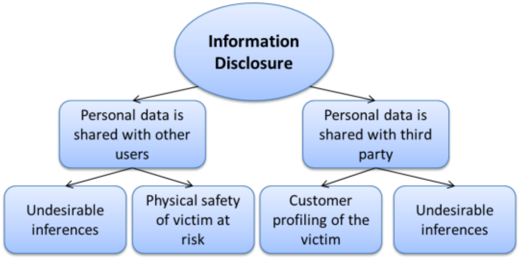

Information Disclosure
Personal data is shared with other users
Personal data is shared with third party
Undesirable inferences
Physical safety of victim at risk
Customer profiling of the victim
Undesirable inferences

Figure 5. Information disclosure privacy threat tree

5.3.2 Privacy threat tree for content unawareness

Figure 6 refers to the privacy threat tree for content unawareness. Content unawareness occurs at the victim level when the victim provides more personal data than is required or does not read the privacy policies. Providing too much personal data is unnecessary and opens up opportunities for further undesirable inferences. There is also the possibility that a victim does not read the privacy policies and therefore is unaware that certain aspects of their personal data is being collected and shared. The victims may be unaware of the purpose for which their personal data is collected, or how it is used. The victims may neither be aware that their personal information is being collected nor their personal data is being shared with third parties. All these situations can result in information disclosure to which the user has unwittingly provided their consent.

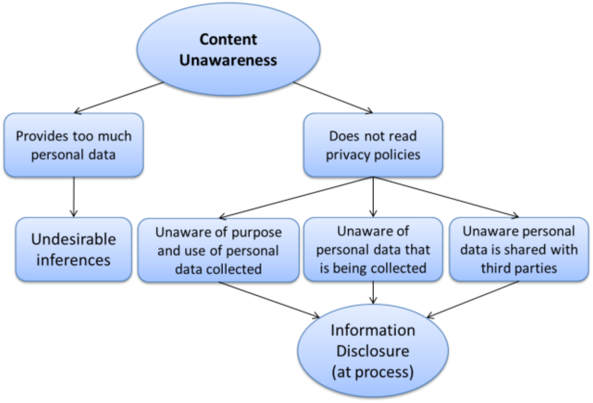

Content Unawareness
Provides too much personal data
Does not read privacy policies
Undesirable inferences
Unaware of purpose and use of personal data collected
Unaware of personal data that is being collected
Unaware personal data is shared with third parties
Information Disclosure (at process)

Figure 6. Content unawareness privacy threat tree

5.3.3 Misuse case scenarios.

In this section, we provide a misuse case scenario of victim's personal information based on the threat tree patterns. The misuse case model is based on the LINDDUN model. The threat trees in Figures 5 and 6 indicate that to be susceptible to the threat of content awareness, the victim either unknowingly provides too much personal data or does not read privacy policies. For information disclosure, the registry forwards the data to a third party or another agent. These are the preconditions of the misuse case. To create the attack scenario, the attacker first needs to have access to the registry (data store), and either the victim (data subject) can be re-identified or the pseudonyms can be linkable. In this scenario, the actions of the misusing actor are actually completely legitimate as outlined in their privacy policy. However, the data use/sharing practices do not comply with the victim's expectations or legislation. Although law 26.827, Article 45, states that the consent of the victim to publish their data and personal information is always required [7], the victim may not be aware of the consequences of making its data public or could not understood the privacy policies. The attack case scenario is presented below.

Title: Misuse Case 1, Content Unawareness and Information Disclosure
Summary: victim unknowingly provides personal data to the agent
Assets, stakeholders and threats: victim's personal information. The victims are unaware the information is collected and sent.
Potential threats: surveillance, secondary use, disclosure, exclusion
Primary misusing actor: victim for not reading privacy policy.
Basic flow:

Victim consents to privacy policy without reading it.

Victim unknowingly sends personal information to the agent.

Alternative flow: Same as the above except that the agent sends victim's personal information to a third party for other purposes.

Trigger: Victim does not read the privacy policy that outlines the agent's privacy practices.

Preconditions:

Victim provides consent but has not read or understood the privacy policies.

Victims have some sort of expectation for privacy, which does not actually correlate with the privacy policy or the data sharing practices of the agent.

5.3.4 Privacy requirements/controls.

Based on the above analysis of threats and illustrative attack scenario, we now propose some privacy requirements and controls needed to mitigate these threats. The IETF outlines in their privacy considerations [16] two major mitigation techniques to deter threats of surveillance, disclosure, secondary use and exclusion. Techniques are data minimization and user participation:

- **Data minimization:** limiting collection, use, disclosure, retention, identifiability, sensitivity, and access to personal data to the minimal amount necessary to perform a task. Reducing the amount of data exchanged reduces the amount of data that can be misused. Data minimization mitigates the threats of surveillance, secondary use and disclosure.
- **User participation**: data collection and use that happens "in secret," without the individual's knowledge, is apt to violate the individual's expectation of privacy and may create incentives for misuse of data. As a result, privacy regimes tend to include provisions to support informing individuals about data collection and use and involving them in decisions about the treatment of their data. In an engineering context, supporting the goal of user participation usually means providing ways for users to control the data that is shared about them. It may also mean providing ways for users to signal how they expect their data to be used and shared. User participation mitigates the threats of surveillance, secondary use, disclosure and exclusion.

Our threat model illustrates that the privacy requirements are data minimization and user participation, in order to mitigate the threats of information disclosure and content unawareness, which can lead to surveillance, disclosure, secondary use and exclusion. Privacy controls, which achieve the goals of data minimization and user participation, include implementing a privacy access control model.

6. Conclusion and future work

In this work, we proposed an approach to investigate the privacy of institutional violence complaints in Argentina. The approach was adapted from existing security and privacy methodologies.

Starting with an overview of the technical architecture, we defined a BPMN process model for registering victims' complaints in a database. This allowed us to identify personal data assets and data flow. Next, we used the LINDDUN methodology to identify privacy threats and threat agents, and illustrated methods of attack through threat trees. This allowed us observing different methods an attacker can use to reach the data and creating misuse case scenarios based on the threat tree patterns.

For the purpose of this paper, we addressed the threats of information disclosure and content unawareness in relation to an individual's privacy when reporting instances of institutional violence. Aiming to minimize these threats, the identified privacy requirements for the proposed process are data minimization and user participation, which can lead to surveillance, disclosure, secondary use and exclusion.

For user participation, it is part of future work to study how to make sure that individuals understand the policy and in which way they could control their own data. Future work is also concerned with analyzing other threat categories such as linkability, identifiability, non-repudiation and detectability. We also plan to implement this process for surveying institutional violence complaints in a business process management system taking into account the identified privacy threats and requirements.

7. Acknowledgements

The authors are grateful to Universidad Tecnológica Nacional (UTN), Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), and Agencia Nacional de Promoción Científica y Tecnológica (ANPCyT) for their financial support. This work was also supported by the São Paulo Research Foundation (Fapesp) under Grants 2015/16615-0 and 2016/00014-0; by the Ministry of Science and Technology (MOST), Taiwan, under MOST Grants: 105-2923-E-027 -001 -MY3, 105-2221-E-027 -113, and 105-2811-E-027 -001; and the Natural Sciences and Engineering Research Council of Canada (NSERC), under NSERC Discovery Grants Program: RGPIN-2016-05023.

8. References

[1] Lessa, F. Beyond transitional justice: exploring continuities in human rights abuses in Argentina between 1976 and 2010. Journal of human rights practice, 3(1), 25-48. 2011.

[2] Bureau of Democracy, Human Rights, and Labor. 2015 Country Reports on Human Rights Practices. United States Department of State. Report. 2016. http://www.state.gov/j/drl/rls/hrrpt/2015/wha/252985.htm.

[3] Ciuciu, I., Zhao, G., Mülle, J., von Stackelberg, S., Vasquez, C., Haberecht, T., Meersman, R. and Böhm, K., 2011. Semantic support for security-annotated business process models. In Enterprise, Business-Process and Information Systems Modeling (pp. 284-298). Springer Berlin Heidelberg.

[4] Hung, P. C. K., and Cheng, V. S. Y. (2009). Privacy, Encyclopedia of Database Systems, Springer, pp. 2136 – 2137.

[5] Alhaqbani, B., Adams, M., Fidge, C.J. and ter Hofstede, A.H., 2013. Privacy-aware workflow management. In Business Process Management (pp. 111-128). Springer Berlin Heidelberg.

[6] Mülle, J., von Stackelberg, S. and Böhm, K., 2011, December. Modelling and transforming security constraints in privacy-aware business processes. In 2011 IEEE International Conference on Service-Oriented Computing and Applications (SOCA) (pp. 1-4). IEEE.

[7] Argentine System of Judicial Information. http://www.apt.ch/content/files/npm/americas/ley268271%20%282%29.pdf. Law 26.827. 2012.

[8] Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. http://www.apt.ch/content/files_res/OPCAT%20English.pdf

[9] van den Braak, S., Choenni, S., & Verwer, S. (2013). Combining and analyzing judicial databases. In Discrimination and Privacy in the Information Society (pp. 191-206). Springer Berlin Heidelberg.

[10] Zuiderwijk, A., Janssen, M., Meijer, R., Choenni, S., Charalabidis, Y., & Jeffery, K. Issues and guiding principles for opening governmental judicial research data. In Electronic Government (pp. 90-101). Springer Berlin Heidelberg, 2012.

[11] OPCAT status – Argentina. http://www.apt.ch/en/opcat_pages/opcat-situation-84/?pdf=info_country. [Accessed on June 2016].

[12] J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan, "Chapter 3: Threat Modeling," in Improving Web Application Security: Threats and Countermeasures, Microsoft Corporation, 2003.

[13] S. Hernan, S. Lambert, T. Ostwald and A. Shostack, "Uncover Security Design Flaws Using the STRIDE Approach," MSDN Magazine, 2006.

[14] van den Braak, S. W., Choenni, S., Meijer, R., & Zuiderwijk, A. Trusted third parties for secure and privacy-preserving data integration and sharing in the public sector. In Proceedings of the 13th Annual International Conference on Digital Government Research (pp. 135-144). 2012.

[15] Debnath, N., Uzal, R., Montejano, G., & Riesco, D. A software application to improve human rights watching activities and to prepare police stations to face the ISO 9001: 2008 certification procedure. In 9th IEEE International Conference on Industrial Informatics (pp. 649-653), 2011.

[16] A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen and R. Smith, "RFC 6973: Privacy Considerations for Internet Protocols," IETF, 2013.

[17] M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen, "A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements," in Interdisciplinary Institute for Broadband Technology (IBBT), Belgium, 2010.

[18] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," TU Dresden and ULD Kiel, 2010.

[19] BPMN. http://www.omg.org/spec/BPMN/2.0/. 2011.

[20] Parks, R., Xu, H., Chu, C.H. and Lowry, P.B., Examining the intended and unintended consequences of organisational privacy safeguards. European Journal of Information Systems, pp.1-29.

[21] Koops, B. and Leenes, R.E. Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law. International Review of Law, Computers & Technology 28 (2), p. 159-171, 2014.

[22] Hoepman, J.H., 2014, June. Privacy design strategies. In IFIP International Information Security Conference (pp. 446-459). Springer Berlin Heidelberg.

[23] Heurix, J., Zimmermann, P., Neubauer, T. and Fenz, S., 2015. A taxonomy for privacy enhancing technologies. Computers & Security, 53, pp.1-17.

[24] Hansen, M., Jensen, M. and Rost, M., 2015, May. Protection goals for privacy engineering. In Proceedings of the 2015 IEEE Symposium on Security and Privacy Workshops.

[25] van Veenstra, A.F. and Ramilli, M., 2011, August. Exploring information security issues in public sector inter-organizational collaboration. In International Conference on Electronic Government (pp. 355-366). Springer Berlin Heidelberg.