Privacy and Transparency within the 4IR: Two faces of the same coin

Bianca Rodrigues Teixeira

Department of Informatics, Pontifical Catholic University, Rio de Janeiro, Brazil
bteixeira@inf.puc-rio.br

Daniel Schwabe

Department of Informatics, Pontifical Catholic University, Rio de Janeiro, Brazil
dschwabe@inf.puc-rio.br

Fernanda A. Baião

Department of Informatics, Pontifical Catholic University, Rio de Janeiro, Brazil
fbaiao@inf.puc-rio.br

Flávia M. Santoro

Postgraduate Program in Computational Sciences, University of the State of Rio de Janeiro, Rio de Janeiro, Brazil
flavia@ime.uerj.br

Maria Luiza M. Campos

Department of Computer Science, Federal University or Rio de Janeiro, Rio de Janeiro, Brazil
mluiza@ppgi.ufrj.br

Leticia D. Verona

Postgraduate Program in Informatics, Federal University or Rio de Janeiro, Rio de Janeiro, Brazil
leticiaverona@ufrj.br

Carlos Laufer

Department of Informatics, Pontifical Catholic University, Rio de Janeiro, Brazil
laufer@globo.com

Simone Barbosa

Department of Informatics, Pontifical Catholic University, Rio de Janeiro, Brazil
simone@inf.puc-rio.br

Sergio Lifschitz

Department of Informatics, Pontifical Catholic University, Rio de Janeiro, Brazil
sergio@inf.puc-rio.br

Rosa Maria E. Moreira

Postgraduate Program in Computational Sciences, University of the State of Rio de Janeiro, Rio de Janeiro, Brazil
rcosta@ime.uerj.br

ABSTRACT

The Fourth Industrial Revolution (4IR) is characterized by a fusion of technologies, which is blurring the lines between the physical, digital, and biological spheres. In this context, two fundamental characteristics emerge: transparency and privacy. From one side, transparency can be seen as the quality that allows participants of a community to know which particular processes are being applied, by which agents, and on which data items. It is generally regarded as a means to enable checks and balances within this community, so as to provide a basis for trust among its participants. Privacy, on the other side, essentially refers to the right of an individual to control how information about her/him is used by others. The issue of public transparency versus individual privacy has long been discussed, and within already existing 4IR scenarios, it became clear that the free flow of information fostered by transparency efforts poses serious conflicting issues to privacy assurance. In order to deal with the myriad of often conflicting cross-cutting concerns,

Internet applications and systems must incorporate adequate mechanisms to ensure compliance of both ethical and legal principles. In this paper, we use the OurPrivacy Framework as a conceptual framework to precisely characterize where in the design process the decisions must be made to handle both transparency and privacy concerns.

CCS CONCEPTS

• Information systems → Social networks • **Information systems → Semantic web description languages**
• Security and privacy → Social aspects of security and privacy

KEYWORDS

Privacy, Transparency, Trust, Semantic Web, Policy, Nanopublications, Knowledge Graph.

1 Introduction

The years of the Third Industrial Revolution (3IR), also called the Digital Age, when digital technologies enabled new ways of generating, processing and sharing information, are ending. According to Klaus Schwab, the founder of the World Economic Forum, we are moving into the Fourth Industrial Revolution (4IR) [12], which builds on 3IR and adds a fusion of technologies, thus blurring the lines between the physical, digital, and biological spheres.

As the daily lives of billions of people are affected – and dependent – on the flow of information (and, ultimately, on knowledge) [14], two important characteristics of the use of such information emerge: transparency and privacy.

Transparency can be seen as the quality that allows participants of a community to know which particular processes are being applied, by which agents, and on which data items. It is generally regarded as a means to enable checks and balances within this community, so as to provide a basis for trust among its participants. If we take the whole society as a community, these checks and balances are reflected on its political system, to prevent misuse by any of the parties involved. Particularly, one of the mechanisms created to increase Transparency in political systems is the enactment of legislation ensuring the right of its members (i.e., citizens in general) to access, create or publish data from a variety of contexts, ranging from the details and results of government acts to consumer-related details of goods and products, as well as the right of individuals to freely create, publish and access information [10].

Privacy, on the other hand, is a basic human right [27], but because of the lack of consensus on its concept, it is difficult to define what it means. Currently, privacy is a comprehensive concept, encompassing freedom of thought, control over the body, isolation, control over personal information, freedom of vigilance, reputation protection and protection against searches and investigations [7]. Theorists have characterized privacy in terms of access [28], or the merit that gives an individual the ability to control access that others have to him/her [1]. Privacy is also defined as the ability to determine when, how, and to what extent information about us is communicated to other people [2]. Despite its several definitions in the literature, it essentially refers to the right of an individual to control how others use information about her/him.

The issue of public transparency versus individual privacy has been long discussed, most particularly Aristotle's distinction between the public sphere of political activity and the private sphere of domestic life. Within already existing 4IR scenarios, it became clear that the free flow of information fostered by transparency efforts poses serious conflicting issues to privacy assurance. In order to deal with the myriad of often conflicting cross-cutting concerns, Internet applications and systems must incorporate adequate mechanisms to ensure compliance of both ethical and legal principles.

In this paper, we use OurPrivacy [5] as a conceptual framework of reference to precisely characterize where in the design process the decisions must be made by designers to handle both transparency and privacy concerns, and how it can support accountability.

2 Background on Transparency and Privacy

According to Meijer [3] and others [14][29][16][19], transparency can be defined as "the availability of information about an actor that allows other actors to monitor the workings or performance of the first actor." It contemplates the "capacity of outsiders to obtain valid and timely information about the activities of government or private organizations" [18].

As a relational concept, transparency presupposes the involvement of an observed and an observer [8]. Besides, there is a difference as to whether the actor that makes information available is an organization or an individual (who may or may not be part of a certain organization) [17] and whether the information relates to an individual or to other more complex events or situations.

Transparency, then, is closely coupled to accountability [25]. However, while transparency is one ingredient in accountability, it is not sufficient. According to Boven [15], accountability essentially means an obligation to explain and justify the conduct of and agent to a third party (the actor and the forum, respectively, in Boven's terminology). Transparency initiatives should provide citizens and other stakeholders with information on the actions of public organizations in order to hold elected officials and public agencies accountable for their decisions and actions. The conceptual complexity of the data openness in the public sector, as opposed to the private sector, relates to several aspects: i) the changing notions of public/private interests; ii) the delicate balance between freedom of information and privacy; iii) government security issues; and iv) the notion that information maintained by the governments is a public asset and should be accountable [24].

Transparency and accountability are also related to privacy. In current business contexts, for example, users/consumers' information plays a central role, supporting sales and marketing strategies, and, most often, strongly influencing and directing consumer behavior. Privacy, in this case, refers to the right of the individual to control how information about him/her is used by others, such as a company. Transparency, on the other hand, supports the enforcement of privacy and other data protection regulations, since the disclosure of information about the company's processes and procedures associated to this individual contributes to trusting that it is indeed compliant with these regulations [17]. As stated by Gutwirth and de Hert [23], data protection and criminal procedures "can be mainly – not exclusively – seen as 'tools of transparency' (regulating and channeling necessary/ reasonable/ legitimate power)" in comparison with privacy, which "is an example of a 'tool of opacity' (stopping power, setting normative limits to power)".

Regulations are important instruments to guarantee rights and duties among involved parties. In general, users' contracts, inter-organizational agreements, domain specific norms and legislation are constantly evolving, reflecting on demands from a changing society, as well as requirements from the adoption of new technologies. The Data Protection Directive of 1995 made no mention to individual rights to data protection, focusing, instead, mostly on controllers' obligations. More recently, the General Data Protection Regulation (GDPR) [21] focuses on "protecting fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data". However, the European Union already had previous regulations concerning privacy, more specifically in the European Convention on Human Rights, which stated the principle that data should only be used for the limited purpose for which it was gathered.

As a data protection regulation, the GDPR imposes greater obligations on actors, taking rights much further [30]. In this context, transparency is explicitly associated to the fact that any request for consent should be intelligible, accessible and expressed in clear language, and forcing disclosure of information about data transfer and use, encompassing a much wider scope than only privacy issues.

Similarly to the GDPR, Brazil has recently approved the General Data Protection Law (abbreviated in Portuguese as LGPD), which will come into effect in early 2020. It is a comprehensive regulation, contemplating also extraterritorial activities involving Brazilian citizens [13]. Its concept of personal data refers to "information related to an identified or identifiable person". It is similar to the GDPR definition, with wording susceptible to a broad spectrum of interpretations. A more important issue, though, is its relation – complementarity and conflict – with the Access to Information Law that came into effect in 2012, and since then has fostered the publication of an extraordinary volume of government data.

Privacy frameworks have been proposed independently of the GDPR. The National Institute of Standards and Technology (NIST), in collaboration with partners from the private and public sectors, is developing a privacy framework, intended to be compatible with US and international regulations. It includes a catalog of issues, focusing on privacy risk management. Another example is the Privacy Control Framework (PCF) of NOREA (Dutch Association of chartered IT-auditors) [20], proposed as a privacy control assessment guide. It contains 104 controls in total, divided over 32 subjects in 9 Lifecycle Management phases. The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) [4] is a certification program designed to ensure the flow of personal information across APEC member borders. These frameworks, although comprehensive, are not intended to propose methods to deal with each privacy issue identified.
As a final observation, we note that privacy is concerned with controlling the use of information related to individual persons, whereas transparency is concerned with controlling the use of a broader set of information, including – but not limited to – information about persons.

3 A Summary of the OurPrivacy Framework

We present here a summary of the OurPrivacy framework, in order to describe the main concepts needed to characterize later the issues to be discussed.
OurPrivacy assumes that the information to be used is stored in a Knowledge Graph (KG), a term introduced by Google in 2012 to denote a graph of inter-related items. Stated another way, a Knowledge Graph represents a collection of interlinked descriptions of entities – real-world objects, events, situations or abstract concepts – where:

- Descriptions have a formal structure that allows both people and computers to process them in an efficient and unambiguous manner;
- Entity descriptions contribute to one another, forming a network where each entity represents part of the description of the entities related to it.[1]

Thus, we define Privacy as "controlled access to information related to some agent", where all the information is stored in a given KG.
Figure 1 shows a diagram of the use of information within a KG, represented by a Request for an Action over an Artifact made by some Actor (henceforth named an Agent). We assume Artifacts contain a set of statements, thus forming a subgraph of the KG. Since Privacy refers to actions over some information, an Authorization must be granted for this Request, according to the Rules set forth by stakeholders. Stakeholders include persons *related to* the artifact, and institutional agents such as "the State" (whose rules are stated as laws). Rules may be based (drawn) on any information available in the KG.
For any Action request there may be several applicable rules, whose evaluation outcomes may result in conflicting Authorization responses. Since the Action request must have a definitive Authorization value, a conflict resolution strategy must be employed to reach a final decision. Such strategy is in turn subject to Governance Rules.
The general conflict resolution process can be expressed by the following algorithm.

1. Given Request(Agent, Action, Artifact),
   Let RS <- RuleSet(Artifact).
2. Let RS <- Sort-by-Precedence(RS, decreasing).
3. Let A <- DefaultAuthorization.
4. For each R in RS,
   a. Let AR <- Eval(R, Person, Action, Artifact);
   b. If AR = "Allowed" or AR = "Denied",
      return AR.
5. return A.

We first give an overall explanation of the algorithm, followed by a thorough discussion of some important details. In line 1, `RuleSet(Artifact)` is a function that computes the set of applicable rules. In line 2, this

[1] https://www.ontotext.com/knowledgehub/fundamentals/what-is-a-knowledge-graph/

`RuleSet` is sorted in a decreasing precedence order, according to some criteria. Line 3 establishes the `DefaultAuthorization` – i.e., "everything is allowed unless denied," or vice-versa. Next, each Rule is evaluated in the sorted order. The evaluation of a rule may result in "`Allowed`", "`Denied`" or "`Nil`" (i.e., undefined). Since the rules are ordered, the first one to obtain a non-Nil value is the Authorization result.
This algorithm abstracts the essential decisions that must be made, in lines 1-3, to wit:

1. Who can formulate a rule for a given artifact?
2. How are conflicts between rules resolved?
3. What are the allowed actions over artifacts?

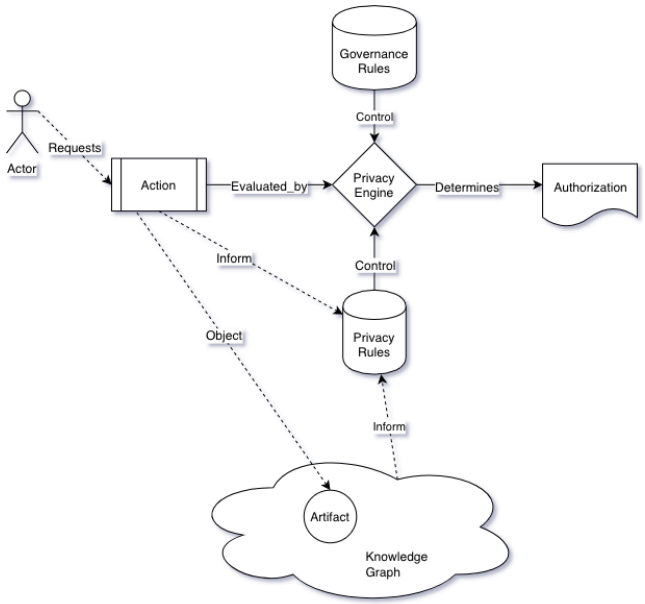

Figure 1: The Privacy Process

We detail possible answers to these questions in the following sub-sections.

3.1 Artifact Representation

We propose to represent an Artifact as a nanopublication[2]. "A nanopublication is the smallest unit of publishable information: an assertion graph about anything that can be uniquely identified and attributed to its author. Individual nanopublications can be cited by others and monitored for their impact on the Community". It is composed of three elements (a.k.a. named graphs): (i) an *assertion graph*, representing a minimal unit of thought that expresses a relationship (i.e., a predicate) between a subject and an object; (ii) a *provenance graph*, representing contextual metadata about the assertion, denoting "how the assertion came to be", including for example methods that were used to generate the assertion, authors, institutions, time-stamps, grants, links to DOIs, and URLs about the assertion; and (iii) a *publication info graph*, representing metadata about the nanopublication as a whole. The publication info differs from the provenance graph since the former pertains to both the assertion and provenance, while the latter relates just to the assertion.
As any nanopublication, an Artifact comprises an *assertion graph*, a *provenance graph* and a *publication info* graph, as follows.
The *assertion* graph will contain a set of assertions about the content of the Artifact, thus enabling the semantic evaluation of the privacy rules. The assertions in this graph are a subset of the assertions in the KG.

[2] http://nanopub.org

Thus, if an Agent posts an image that depicts some event, it would have statements about the participants and their roles, location information, date information, etc. as assertions in the assertion graph. We do not discuss here how such assertions containing semantic information are obtained (extracted) from the representation (image, video, text).
The *provenance* graph of the Artifact will contain provenance information about the assertions in the assertion graph (e.g., what image or natural language processing software was used, recorded location info, whether the assertions were inferred using some inference engine, etc.). The provenance graph can be used to represent, to the desired level of detail, the supporting information for the assertions. For example, if an automated face recognition algorithm was used, the provenance information represented in the *provenance* graph of the nanopublication may inform which algorithm, which parameters were used in this particular case, and a confidence factor. In the case of a rule stated by a person that has legal authority over another (e.g., a parent over a child), the provenance information can include supporting evidence to establish such legal authority (e.g., a reference to a birth certificate that states that rule author is indeed the parent of child depicted in the photo).
The *publication info* graph will contain metadata about the creation of the Artifact itself, such as its creator.

3.2 Rules

The first decision is to determine what the applicable rules are given an Artifact, defined in the `RuleSet(Artifact)` function. This leads to the question "who has the right to define a Privacy Rule that controls actions over this artifact?" The definition itself indicates that it must be any agent that is somehow *related* to the information contained in the artifact; but, stated in this way, it is too general. Any useful instantiation of the framework must spell out such relation types, which can include:

- Any agent directly identified in the artifact – for example, some person appearing in a posted photo or video;
- Any agent referred to (mentioned) in the artifact – for example, some person cited in a post;
- The creator of the artifact;
- Any agent related to the creation of the artifact – for example the author of a video posted by someone else;
- Any agent who has legal jurisdiction over an agent identified or mentioned in the artifact;
- The legal system(s) that has(have) jurisdiction over the KG, the agent or the action request.

The presence of such relations can directly occur in the KG (i.e., as a typed edge), or as a composition of valid relations. Furthermore, the rules may (or may not) allow the use of inferred relations in the KG.
Rules are of the form antecedent => consequent, both of which are sets of statements [26]. The antecedent of privacy rules may refer to any statements in the KG, including

- Any statements in the graphs in the artifact's nanopublication (including provenance information);
- The identity of the agent requesting permission;
- The type of action;
- Information in the KG serving as contextual information), such as
    - Date/time of the request;
    - Current location of agents involved;

Rules are themselves Artifacts, so they are nanopublications. The actual specification of the rule is given in its assertion graph, using a notation such as N3Logic [26] or SWRL[3]. Governance Rules are Rules that include other Rules (in either antecedent or consequent), so in this sense they are meta-rules.
Governance rules can be used to express precedence relations between rules, and to capture certain aspects of the privacy process. A metarule can, among other things, control the creation of any rule. This can be used

[3] https://www.w3.org/Submission/SWRL/

to precisely control, for example, what are the relation types allowed to be considered when computing the generic concept of "information *related* to a person" in the definition of Privacy. The example below illustrates how one can restrict privacy rules to refer only to PersonalInformation (assuming the default authorization value is "Denied").

KG

PrivacyRule subClassOf Rule.

{?KG log:semantics ?KGS;
?KGS log:includes {?p1 ?r ?p2.
(?p1 rdf:type Person OR ?p2 rdf:type Person)}} => {?r rdf:type PersonalInformationRelation}

Meta Rule1

{?r1 type PrivacyRule, antecedent ?Ant. ?Ant log:semantics ?AS. ?AS log:includes {?p1 ?r ?p2}. ?r rdf:type PersonalInformationRelation}, ?act rdf:type Create, object:?r1}
=>{<at> type:authorization, rule <MRule1>, action <?act> , value "Allowed"}

The OurPrivacy Framework can be applied for transparency rules as well by simply allowing rules to refer to Artifacts of any kind, and not only Persons. This will be illustrated in the examples in Section 4.

The provenance information and the publication info associated to a metarule nanopubulication can provide support for accountability. The provenance sub-graph can include reference(s) to the pertinent legislation, as well as legal cases that support the interpretation encoded in the rule, and the publication info subgraph contains information about the rule author.

3.3 Conflict resolution

In the conflict resolution algorithm, the enabled rules are sorted in descending precedence order in the `Sort-by-Precedence(RS, decreasing)` function call. Given that, in general, many applicable rules regarding the authorization for the intended action may exist, it is possible that two different rules give mutually exclusive authorizations. This is resolved using a sorting function that typically combine several types of information to establish order relations between rules.

Several possible complementary order relations that can be employed, such as:

- Establish a hierarchy between users – rules defined by a higher-ranked user take precedence over rules defined by lower-ranked ones. For example, rules established by laws take precedence over rules stated by individuals;
- Establish a hierarchy over the relation types. Rules defined by users related to the artifact through a higher-ranked relation type take precedence over rules defined by users related to the artifact via a lower-ranked relation type. For example, one may state that "identification" takes precedence over "mentioning". Thus, in a video where a person A is identified, and person B is mentioned in a conversation, person A's rules would take precedence over person B's rules.
- Since hierarchies are partial orders, they may not completely define precedence, so further conflict resolution strategies are still needed. Such and Criado [11] identified six categories of strategies that can be employed. Most require user involvement at runtime, but the aggregation-based class can be easily incorporated into an algorithm. Strategies in this class define an aggregation function such as consensus, majority, minimum fixed number of votes, permit-overrides, deny-overrides, etc. – see also [9] – and replace the set of conflicting rules by a single aggregated result;

An alternative to the aggregation approach is to decompose the artifact into finer-grained elements so that each is subject to only one rule. This makes sense when the Action to be performed can be performed on each element independently, such as blurring the face of a given person in a group photo.

4 Example Scenarios and discussions

4.1 Transparency x Privacy

The first scenario regards the Brazilian Transparency Law, which states that information of public interest should be openly released. In this example, P1 is a congressperson and P2, a non-public person who financially contributed to P1's campaign. P1 formulated a rule (Rule 1) that would protect his contributions by allowing only government organizations to have access to them, i.e., the general public would not have permission to access them.

Nonetheless, because P1 is a congressperson, the Law of Transparency demands her/his campaign information to be publicly available. Given that laws have precedence over personal rules, the Rule representing the Law of Transparency (Rule 2) precedes Rule 1. The following statements and rules characterize this scenario, where we assume the default authorization is "`Denied`".

KG

Read subClassOf Action.

<t> type Transaction, recipient <P1>.

<t> type PublicInterestInformation.

Rule 1.

{?T type Transaction; assertions ?Assrt. ?Assrt log:semantics ?AS. ?AS log:includes {?T category <CampaignContribution>. <act> type Read; object ?T. ?Org intends <act>, org:subOrgOf <Government>. ?T author <P1>}

=> {<at> type Authorization, rule "Rule1", action <act>, value "Allowed"}

Rule 2.

{?pi type PublicInterestInformation. <act> type Read; object ?pi. ?Agent intends <act>}

=> {<at> type Authorization, rule "Rule2", action <act>, value "Allowed"}

The Transaction object `?T` representing the campaign contribution has the type `PublicInterestInformation` in the Knowledge Graph. According to Rule 2, which precedes Rule 1, everyone who intends to read such information should be allowed to do so.

A slightly different situation arises when P1 is actually the brother of P2, for example. This family relationship can be protected by the Brazilian Data Protection Law, which covers personal data (Rule 3). The `siblingOf` relationship in this case is personal information, but it can also be regarded as public interest information. This entails a discussion on whether public interest information precedes personal data protected by the Brazilian regulation, as it is unclear which law should be applied.

The fact that P1 is sibling of P2 may not be public knowledge, or present in the KG, but the fact that P2 contributed to P1's campaign is. So, does the fact that they are siblings matter in this case? The General Data Protection Regulation states an individual can restrict actions on his/her personal information. If there is a public interest information involved, such as the financial contribution, then should other personal information become that of public interest, and thus subject to the transparency legislation?

In the statements below, we consider the sibling relationship as being both personal information and public interest information, which would then generate direct conflict based on Rule 2, stated above, and Rule 3, below.

KG

Read subClassOf Action.

<t> type Transaction, recipient <P1>.

<t> type PublicInterestInformation.

<P1> siblingOf <P2>

<siblingOf> type rdf:Property, PersonalInformation, PublicInterestInformaton.

Rule 3.
{?pi type PersonalInformation. <act> type Read; object ?pi. ?Agent intends <act>}
=> {<at> type Authorization, rule "Rule3", action <act>, value "Denied"}

Taken separately, Rule 2 and Rule 3 may act as default rules, in terms of the conflict resolution algorithm. Default rules are superseded when a more specific rule precedes the default rule. However, in this example these two rules are in conflict with one another. The precedence between them is arguable, because, as discussed, it is unclear whether personal information precedes public interest information or vice-versa. Hence, whether the `siblingOf` relationship between P1 and P2 could be acted upon or not depends entirely on the implementation of the `Sort-By-Precedence` function.

4.2 Ensuring transparency for public citizens: The right to be forgotten case

This example takes place on Twitter and features a famous person or politician, such as the President of Brazil – Jair Bolsonaro – as the main participant. Imagine a citizen called Lucas, who automatically captures Bolsonaro's tweets and re-posts them on his Twitter timeline. If Bolsonaro deletes a tweet he had previously posted, Lucas will still have the original tweet published on his timeline.

This raises an interesting question regarding the right to be forgotten. Would it be possible for someone (in this case, Bolsonaro) to specify a rule that would prevent others (in this case, Lucas) from re-posting his tweets? Is it legitimate that a user prevents others from sharing his/her own words, or pictures, especially if they have been deleted? Also, in a social network setting, it is virtually impossible to track when users copy and paste a text, or download and upload an image, without referring to the original content.

The possible solutions may also be deemed controversial. It is still not clear whether a public citizen such as Bolsonaro should have the ability to prevent some other user from publishing his original content. Moreover, the right to be forgotten is not guaranteed when it is possible for users to manually re-post tweets or posts.

KG
Read subClassOf Action.
<tw1> type Tweet, author <JairBolsonaro>.
<tw2> type Tweet, author <Lucas>, copyOf <tw1>.
<JairBolsonaro> type PublicFigure.

Rule 1.
{?T type Tweet; <act> type Read, object ?T. ?Person intends <act>.
?T author <JairBolsonaro>}
=> {<at> type Authorization, rule "Rule1", action <act>, value "Denied"}

Rule 2.
{?T1 type Tweet; <act> type Read, object ?T1; ?Person intends <act>.
?T type Tweet; ?T copyOf ?T1. ?T1 author <JairBolsonaro>}
=> {<at> type Authorization, rule "Rule2", action <act>, value "Denied"}

Rule 3.
{<act> type Read. ?Person intends <act>.
?T type Tweet, author <Lucas>}
=> {<at> type Authorization, rule "Rule3", action <act>, value "Allowed"}

Rule 1's antecedent includes the `author` property, indicating that this property is understood as a valid "related to" instance with respect to the definition of privacy. Although not shown, this would be stated in a meta-rule that allows creating rules with this property in its antecedent. By this rule, Jair Bolsonaro has denied Read actions on any of his tweets. We assume Jair Bolsonaro has established this rule at a moment in time after Lucas has copied his tweets, producing the same effect as deleting the tweets (at least for the purposes of the example).

Similarly, by Rule 2, the use of the composition of `author` and `CopyOf` properties in its antecedent expresses the understanding that a copy of someone's tweet is "related to" its original author, and therefore

<JairBolsonaro> is entitled to establish it as a privacy rule. Thus Rule 3 denies Read actions on any copy of his tweets.

Rule 3 (established by Lucas) simply states that all his tweets can be read by everybody. If the default Authorization in this scenario is "Allowed", this rule would be redundant.

In addition to these rules, assume the KG has the statements shown under "KG". If a person intends to read tw2, Rule 2 will return a "Denied" authorization, whereas Rule 3 will return an "Allowed" authorization.

If it is interpreted that a public figure is not protected under the Right to be Forgotten law, since Jair Bolsonaro is a public figure, then Rules 1 and 2 would not be allowed to be created by the Governance Rules, and Rule 3 would prevail. Conversely, if this tweet is, for example, about an offense that he made to someone in the past, it could be considered a proof of a crime. In this case, another rule (based on the Law) would prevail. So, do we (public persons or not) really have the right to be forgotten?

In a scenario where there are no such laws, other criteria may be reflected in the conflict resolution rules. For instance, based on an interpretation of the privacy legislation, Rule 2 would precede Rule 3, and the read action would be denied.

4.3 Privacy issues on digital memories: The Black Mirror case

Futuristic television series *Black Mirror*[4] presents interesting scenarios of privacy invasion. In "The entire history of you", the final episode of the first season, which first aired on December 2011, people use a device called Grain, which is a memory implant that records everything their eyes see, making it possible to browse through previous memories as if they were videos. The main character of the episode, Liam, threatens other people's security to gain access to old memories stored on their Grain [6]. Liam pressures his wife, Ffion, into showing him a memory she has of a sexual affair she had during their marriage. In the episode, she tries to delete the memory, but he notices it and violently prevents the deletion.

In this scenario, Ffion has no protection over her memories. Although she is the one who actively controls the system, if threatened, there is no mechanism that blocks or prevents unwanted access. With OurPrivacy, though, her privacy could be sustained with the help of rules.

For this example, it would make sense for Ffion to write a rule preventing her husband from accessing memories of her love affair (Rule 1). We can consider that each piece of memory is a nanopublication. Since all memories are recorded by the same device, at least part of the provenance information should be the same. The date, time and location, however, will change accordingly.

In Ffion's rule for this example, the assertion graph is key. She is concerned about memories of her affair, which means that memories containing romantic or sexual events with her lover should not be accessed by Liam, her husband. The content of each memory is stated in its assertion graph. Because of that, when Liam states that he wants to see a specific memory – which, in our framework, is an action –, the system checks in the assertion graph of that memory if it contains any mention of a sexual or romantic event with Ffion's lover. If it does, because of Ffion's rule, Liam is denied access to that memory.

Rule 1.

{?M type Memory; assertions ?Assrt. ?Assrt log:semantics ?AS. ?AS log:includes {<Jonas> sexualActWith <Ffion>}. <act> type Read, object ?M. <Liam> intends <act>.

?M author <Ffion>}

=> {<at> type Authorization, rule "Rule1", action <act>, value "Denied"}

Because Ffion is the author of the memories in question, she has the capability of writing rules about them. However, since she is married to Liam and memories of infidelity can directly affect their marriage, it can be debated whether Liam should have the ability to write rules concerning these memories as well. This would cause a conflict, as the values of the ultimate authorization would differ. Liam's rule of wanting access to Ffion's adultery would directly clash with Ffion's rule that prevents Liam's access.

[4] https://www.netflix.com/title/70264888

If the couple had any sort of prenuptial agreement or other type of contract that contained an article regarding infidelity, this document could be used as a conflict resolution artifact. Legal papers can play a great part in our framework, acting as a means to solve conflicts according to the implementation of the `Sort-by-Precedence` function, as discussed in Section 2.

If the prenuptial agreement in question contained a specific stipulation of what would happen to the couple's memories in case of adultery, this could be translated into Rule 2. The clause is that, in case of Ffion having sexual relations with a person other than Liam, and Liam wanting to see that memory, Liam would be allowed to do so.

KG

Read subClassOf Action.

<m1> type Memory, author <Ffion>.

<prenup> type LegalDocument, author <Lawyer1>

Rule 2.

{?M type Memory; assertions ?Assrt. ?Assrt log:semantics ?AS. ?AS log:includes {?Person sexualActWith <Ffion>}. ?Person differentFrom <Liam>. <act> type Read, object ?M. <Liam> intends <act>. ?M author <Ffion>. "Rule2" provenance ?Prov; ?Prov log:semantics ?PV. ?PV log:includes {?prenup type prov:Entity, LegalDocument}}

=> {<at> type Authorization, rule "Rule2", action <act>, value "Allowed"}

Rule 1 and 2 have a clear conflict. Given the legal framework, and the fact that Rule 2's provenance is a legal document, Rule 2 precedes Rule 1, and thus the conflict resolution algorithm will return "`Allowed`" for the authorization request.

5 Conclusions

This paper illustrates the use of OurPrivacy as a framework of reference to address two issues that are commonly taken as contradictory: that of public transparency versus individual privacy We show that, essentially, they refer to opposite sides of the same Quality spectrum and, therefore, may be accounted as two faces of the same coin.

We use the OurPrivacy Framework as a conceptual framework of reference to precisely characterize where in the design process the decisions must be made to handle both transparency and privacy concerns, and how it can support accountability. We show and discuss several real-life scenarios, which evidence this conclusion.

As counter-intuitive as it may seem at first, this is a very interesting conclusion, which may impact the definition of common mechanisms to ensure compliance of both issues without leading to contradictory and non-viable scenarios.

We emphasize that, in its current stage as a conceptual framework, this work does not address concerns with implementation. One of the main goals is to provide support on how to assess the trade-off between privacy and transparency through a sort-by-precedence rule. In this sense, the framework can use any strategy already proposed in the literature, as so, we do not claim to propose a new strategy of conflict resolution.

As the interplay between rules can become quite complex, as future work, we envisage developing a simulator based on OurPrivacy to help designers anticipate the impact of their decisions using the framework, in a way similar to [13].

The issues and concerns raised with OurPrivacy must be dealt with in any implementation. This poses significant challenges that we are already addressing as part of ongoing and future work.

ACKNOWLEDGMENTS

Daniel Schwabe and Flávia Santoro were partially supported by a grant from CNPq.

REFERENCES

[1] Adam D. Moore. 2003. Privacy: Its Meaning and Value. *American Philosophical Quarterly* 40, 3 (2003), 215–227.

[2] Alan F Westin. Privacy and Freedom. Washington and Lee Law Review 25, 1, 16.

[3] Albert Meijer. 2013. Understanding the Complex Dynamics of Transparency. Public Administration Review 73, 3 (2013), 429–439. DOI:https://doi.org/10.1111/puar.12032
[4] APEC Cross Border Privacy Enforcement Arrangement. Retrieved February 27th 2019 from https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Enforcement%20Arrangement.pdf
[5] Bianca Rodrigues Teixeira, Daniel Schwabe, Fernanda Baião, Flavia Maria Santoro, Carlos Laufer, Sérgio Lifschitz, Rosa M. Costa2 Simone D. J. Barbosa. 2019. OurPrivacy: A Framework for Privacy in Social Media, submitted for publication, WWW Journal.
[6] Bianca Rodrigues Teixeira and Flávia Maria Santoro. 2017. Memory and Privacy in The Entire History of You. In Proceedings of Workshop Re-coding Black Mirror 2017 Workshop - 16th International Semantic Web Conference (ISWC 2017).
[7] Daniel J. Solove. 2010. Understanding Privacy (2/28/10 edition ed.). Harvard University Press, Cambridge, MA.
[8] Ethan S. Bernstein. 2016. Making Transparency Transparent: The Evolution of Observation in Management Theory. ANNALS 11, 1 (October 2016), 217–266. DOI:https://doi.org/10.5465/annals.2014.0076
[9] Federica Paci, Anna Squicciarini, and Nicola Zannone. 2018. Survey on Access Control for Community-Centered Collaborative Systems. ACM Computing. Surveys. 51, 1 (January 2018), 6:1–6:38. DOI:https://doi.org/10.1145/3146025
[10] George Ritzer. 2008. Transparency in Global Change: The Vanguard of the Open Society by Burkart Holzner and Leslie Holzner. American Journal of Sociology 114, 1 (July 2008), 267–269. DOI:https://doi.org/10.1086/592526
[11] Jose M. Such and Natalia Criado. 2018. Multiparty Privacy in Social Media. Commun. ACM 61, 8 (July 2018), 74–81. DOI:https://doi.org/10.1145/3208039
[12] Klaus Schwab. 2017. The Fourth Industrial Revolution. Currency, New York.
[13] Manoel Pereira Junior, Simone Isabela de Rezende Xavier, and Raquel Oliveira Prates. 2014. Investigating the Use of a Simulator to Support Users in Anticipating Impact of Privacy Settings in Facebook. In Proceedings of the 18th International Conference on Supporting Group Work (GROUP '14), 63–72. DOI:https://doi.org/10.1145/2660398.2660419
[14] Manuel Castells. 2000. The Rise of the Network Society (2nd ed.). Blackwell Publishers, Inc., Cambridge, MA, USA.
[15] Mark Bovens 2007, Analysing and Assessing Accountability: A Conceptual Framework. European Law Journal 13, 4 (2007) 447-468.
[16] Mathias Klang and Andrew Murray. 2005. Human Rights in the Digital Age. Psychology Press.
[17] Maximilian Heimstädt and Leonhard Dobusch. 2018. Politics of Disclosure: Organizational Transparency as Multiactor Negotiation. Public Administration Review 78, 5 (2018), 727–738. DOI:https://doi.org/10.1111/puar.12895
[18] Michael Johnston. 2014. Transparency. Encyclopedia Britannica. Retrieved February 4, 2019 from https://www.britannica.com/topic/transparency-government
[19] Michael Schudson. 2015. Politics and the Culture of Transparency. In The Rise of the Right to Know. Harvard University Press, Cambridge, MA, 1945–1975.
[20] NOREA Guide Privacy Control Framework - Control objectives and controls for privacy audits and privacy assurance engagements. Retrieved February 27th, 2019 from https://www.norea.nl/download/?id=4160
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[22] Renato Monteiro. 2018. The new Brazilian General Data Protection Law — a detailed analysis. International Association of Privacy Professionals. Retrieved February 4, 2019 from https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/
[23] Serge Gutwirth, and Paul De Hert 2007. Privacy, Data Protection and Law Enforcement - Opacity of the Individual and Transparency of Power. Privacy and the Criminal Law, Erik Claes, Antony Duff, and Serge Gutwirth. eds., Antwerpen-Oxford: Intersentia, 61-104.

[24] Sharon S. Dawes and Natalie Helbig. 2010. Information Strategies for Open Government: Challenges and Prospects for Deriving Public Value from Government Transparency. In Electronic Government (Lecture Notes in Computer Science), 50–60.
[25] Thomas N. Hale. 2008. Transparency, Accountability, and Global Governance. Global Governance 14, 1 (2008), 73–94.
[26] Tim Berners-lee, Dan Connolly, Lalana Kagal, Yosi Scharf, and Jim Hendler. 2008. N3Logic: A Logical Framework for the World Wide Web. Theory Pract. Log. Program. 8, 3 (May 2008), 249–269. DOI:https://doi.org/10.1017/S1471068407003213
[27] United Nations, Universal Bill of Human Rights, Resolution A/RES/217(III)[A]. Retrieved February 4, 2019 from http://unbisnet.un.org:8080/ipac20/ipac.jsp?session=14O243550E15G.60956&profile=voting&uri=full=3100023~!909326~!67
[28] W. A. Parent. 1983. Privacy, Morality, and the Law. Philosophy & Public Affairs 12, 4 (1983), 269–288.
[29] William H. Dutton. 2009. The Fifth Estate Emerging Through the Network of Networks. Prometheus 27, 1 (2009), 1–15.
[30] Yvonne McDermott. 2017. Conceptualising the right to data protection in an era of Big Data. Big Data & Society 4, 1 (June 2017), 2053951716686994. DOI:https://doi.org/10.1177/2053951716686994