DPIA in context: applying DPIA to assess privacy risks of cyber physical systems.

HENRIKSEN-BULMER, J., FAILY, S. and JEARY, S.

2020

future internet

MDPI

Article

DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems

Jane Henriksen-Bulmer *,† **, Shamal Faily** † **and Sheridan Jeary**

Department of Computing & Informatics, Bournemouth University, Fern Barrow, Poole BH12 5BB, UK; sfaily@bournemouth.ac.uk (S.F.); sherryjeary@gmail.com (S.J.)

* Correspondence: jhenriksenbulmer@bournemouth.ac.uk

† These authors contributed equally to this work.

Received: 9 March 2020; Accepted: 18 May 2020; Published: 24 May 2020

Abstract: Cyber Physical Systems (CPS) seamlessly integrate physical objects with technology, thereby blurring the boundaries between the physical and virtual environments. While this brings many opportunities for progress, it also adds a new layer of complexity to the risk assessment process when attempting to ascertain what privacy risks this might impose on an organisation. In addition, privacy regulations, such as the General Data Protection Regulation (GDPR), mandate assessment of privacy risks, including making Data Protection Impact Assessments (DPIAs) compulsory. We present the DPIA Data Wheel, a holistic privacy risk assessment framework based on Contextual Integrity (CI), that practitioners can use to inform decision making around the privacy risks of CPS. This framework facilitates comprehensive contextual inquiry into privacy risk, that accounts for both the elicitation of privacy risks, and the identification of appropriate mitigation strategies. Further, by using this DPIA framework we also provide organisations with a means of assessing privacy from both the perspective of the organisation and the individual, thereby facilitating GDPR compliance. We empirically evaluate this framework in three different real-world settings. In doing so, we demonstrate how CI can be incorporated into the privacy risk decision-making process in a usable, practical manner that will aid decision makers in making informed privacy decisions.

Keywords: contextual integrity; privacy; risk; Data Protection Impact Assessment; DPIA; General Data Protection Regulation; GDPR

1. Introduction

Cyber Physical Systems (CPS) are "integrations of computation and physical processes" [1]. Thus, CPS can combine human, physical and technological components and allow these to communicate seamlessly to derive value (see Figure 1). The value generated will depend on the perspective of the user. For example, for the individual who uses their smart phone to communicate with their heating system, the value will be in having a warm home when they get there. For the electricity company, the value may be in providing the power needed on-demand. In addition, the electricity company may also derive value from, for example, being able to remotely read the customer's meter, or use the data generated to predict when the customer will next need additional power to be supplied. However, this also raises a number of security and privacy concerns that need to be explored and addressed.

While a lot of research has been done around what the security threats, vulnerabilities and implications of CPS might be [2], most of this work considers privacy only as a sub-set of security considerations [3]. We contend that privacy must be considered in its own right and on a more holistic basis. Some work has been done in this area, discussing how privacy might be affected by the use of CPS and highlighting the need for improved decision making to ensure privacy is preserved

in CPS [4], a notion that we subscribe to. We contend that, not only does privacy need to be discussed, a practical framework for how to do this in a holistic manner, is also sorely needed.

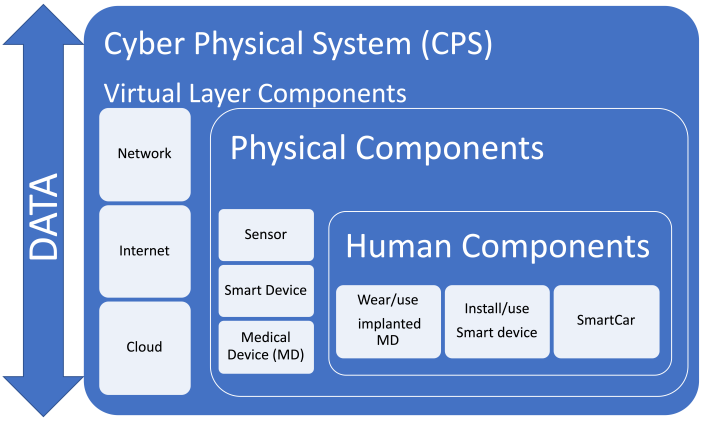

Figure 1. Cyber physical system components.

This paper seeks to address this gap by introducing the DPIA Data Wheel, a privacy risk assessment framework devised for supporting informed decision making around privacy risk and conducting Data Protection Impact Assessments (DPIA) for any system, project or scenario that involves *high risk* processing of data. This, we contend, will include most CPS.

Contribution

The creation of the DPIA Data Wheel came about as part of an action intervention study conducted to guide a local Charity in the UK through implementing the changes brought in by the General Data Protection Regulation (GDPR) across the organisation [5]. As part of this implementation, a number of complimentary elements arose, including a need for a privacy risk assessment that would allow the organisation to assess the privacy implications of their data processing on their customers in a consistent, repeatable manner, allowing them to meet their obligations for conducting DPIAs under Article 35 of GDPR [6]. This paper discusses this complimentary element, and provides a detailed explanation for how this DPIA framework was created, and the considerations taken into account in the design.

The findings from this study showed that including contextual questions in a practical guided manner within the privacy risk assessment, helped raise awareness of not only what is meant by context in terms of privacy risk assessment, but also identified contextual nuances that might not otherwise be apparent when conducting traditional privacy impact assessments (PIAs). However, to ensure these aspects are understood by assessors, in-depth training will need to be provided to ensure they appreciate and know how to assess privacy risk in context, this is discussed in Section 7. Further, the results show that for optimum contextual consideration to be included in the privacy risk assessment, it is advisable to consult with a wide range of stakeholders as part of the consultation process. This also widens the scope for more privacy risks to be identified and included in the privacy risk assessment. We also found that while organisations are comfortable assessing risks from an organisational perspective, they struggled to appreciate that the DPIA requires them to consider risks from the perspective of their customers or service recipients and what this means in practice (see Section 7.1).

In presenting the DPIA Data Wheel, three contributions are presented. First, we provide an exemplar model for how Contextual Integrity (CI) can be used in practice, to ensure context is included as standard, within the privacy risk assessment process, from the perspective of both the organisation and their service recipients. Second, we provide organisations with an empirically evaluated, repeatable, consistent approach to privacy risk assessment, that will facilitate users in assessing the privacy risks associated with any CPS likely to involve high risk data processing,

and identify suitable mitigations for each privacy risk identified. Third, we show how, by using the DPIA Data Wheel, organisations can use the privacy risk assessments created, towards demonstrating compliance with the GDPR.

The rest of this paper is organised as follows. Section 2 explains the background to the creation of a practical DPIA framework. Next, in Section 3, the underpinning concepts and work upon which this DPIA framework was created are outlined, and we explain how CI was used to create a DPIA framework for assessing privacy risks to the individual. This DPIA framework was designed using concepts devised in a pilot study, CLIFOD (Section 3.1), and aligned with official guidance (Section 3.2). The design of the DPIA Data Wheel itself is provided in Section 4. Section 5 explains how this framework was empirically evaluated in three different practical environments, using real data. This is followed by a review of related work in Section 6. We then discuss the outcomes of the evaluations in Section 7 before concluding in Section 8 by re-iterating and reflecting on the contributions made to the wider community.

2. Background

2.1. CPS and Organisational Decision-Making

CPS consist of the integration of physical hardware (e.g., sensors or smart devices) and IT systems that communicate and interact seamlessly via the internet with possible intervention from people to either inject, interact or use the data generated to derive value for themselves or the organisation (see Figure 1). However, the commercial value of such data is content dependent. For example, some businesses use data interpretation and analytics to derive all manner of insight to serve their particular purpose [7]. Once data has been analysed and interpreted, it turns into information which may be interpreted and form the basis of business decisions [8]. Thus, while interpreting data to make decisions is necessary, this in itself is not sufficient; how the data is used, which pieces of hardware, IT systems, processes and people are involved, and the context of such data use must all be taken into account for those decisions to be of value. Moreover, with the introduction of new legislation in recent years, such as GDPR within Europe, additional obligations have been placed on organisations to consider privacy as part of their decision making and, with this, a need for a framework that can be used to apply a more holistic privacy risk assessment to the data generated by CPS and the people who work with them has emerged.

To provide some context, if we consider the individual who interacts with a CPS system using a smart devices (e.g., SmartPhone) to control another smart device remotely (e.g., heating sensors), this interaction will generate data. This data, to the user, may not be of much value, yet, in the hands of commercial organisations or indeed unauthorised threat actors, such data can be very valuable. For instance, for the organisation that wishes to determine how much electricity a customer will need, they may profile that customer based on their previous usage patterns generated by their SmartMeter (another CPS device) [9]. The introduction of GDPR, however, requires that such analysis is no longer viable without first considering the privacy in context, i.e., the use (*processing*) of the data and how this might affect the data subject's privacy [4,6].

2.2. CPS and Privacy

Privacy has many facets; everyone perceives privacy in their own unique way, and privacy tolerances vary from one person to the next. For example, what constitutes an attack on privacy? Historically, the tagging clothing to enable identification of someone's whereabouts has been considered an invasion of privacy [10], yet, many people do not consider allowing their Smart Meter to update their supplier on usage an invasion of privacy, despite the fact that this data could, in the wrong hands, also be used to pinpoint their home location, or establish their preferences [9]. Thus, privacy is more nuanced than a simple public/private dichotomy.

Privacy is difficult to define and, therefore, difficult to design into systems, processes or decision-making. This problem becomes even more difficult to address with CPS that traverse modern technology and physical systems, that traditionally did not have internet connectivity, such as industrial control systems, national infrastructure and smart objects, because of the multiple disparate elements that need considering. CPS can be used to transfer data from physical devices, such as smart meter sensors, via the internet to send usage or location data to be monitored to control systems that can then be used to, for example, monitor performance [11]. This interaction however, gives rise to a number of security and privacy concerns that need to be explored and addressed. Moreover, with CPS, the boundaries between the three disparate elements, the physical, the human and the machine, can be difficult to distinguish and, therefore, privacy considerations become more complicated to assess.

GDPR obliges organisations to reconsider how they use and make decisions around data, with failure to comply giving rise to large monetary fines of up to 20 million Euro [6]. This means that organisations must reconsider practices such as establishing customer preferences from their purchasing history, without first assessing the privacy risks associated with such use of the data. This means that, whereas historically, conducting risk assessment for privacy has been advisable, GDPR has made this a mandatory obligation, requiring organisations to assess the privacy risk for any *"high risk"* data processing activities [12]. Moreover, such privacy risk assessment must be conducted from the perspective of the service recipient or customer (*the data subjects*), rather than the organisation (Article 35, GDPR). Therefore, the organisation who wishes to profile their customers, need to consider the whole cyber-physical process involved in such data use, as part of their decision making. This should encompass both the physical and technological processes, and systems that the data crosses as part of the analysis, in order to gain a complete picture of the potential privacy risks.

While the safety and security risks of CPS have been considered [13], and the security threats, vulnerabilities and implications has been discussed extensively [2], including how privacy may be affected as a result of CPS [3], what most of these papers have in common is that they consider privacy as one component part of the security consideration, rather than as an overarching consideration across the whole of the CPS areas, the physical, the technological and the human in a holistic manner. This, therefore, requires privacy risk to be assessed in context, taking into account the human, technical and physical components of CPS and how these interact to generate data and, thus, value.

One study does discuss privacy to consider how the new provision of GDPR might apply and affect CPSs (or IoT devices), and what this is likely to mean for organisations who operate and use CPSs [4]. This study identifies four challenges in ensuring the data subjects (a.k.a. "users") privacy is maintained and preserved: consent; trust, honesty and transparency; inference, profiling and discrimination; and context-sensitive sharing of identity and how this may be controlled and suggests that one of the ways this can be addressed it to conduct DPIAs that evaluate the risks of processing data and proposes solutions for how to mitigate any risks identified [4].

2.3. Contextual Integrity

To this end, we used Nissenbaum's Contextual Integrity (CI) framework, to underpin the DPIA Data Wheel. The CI framework provides a *theoretical* privacy framework that seeks to address the challenge of how to incorporate context in privacy risks assessments, intended to be a predictive tool for eliciting reactions to changes in information flows, rather than a prescribed method for applying CI in practice ([14], p. 150).

CI involves looking at data flows and how any alterations in the way data is conveyed or shared might affect privacy. Decision makers are asked to not only consider the data being processed, but also consider the people involved ('the actors'), their roles (e.g., as data processors and as individuals), and how the data flows between actors. CI also asks that the surrounding context be considered to account for the values, norms, purposes and expectations of the actors and how this might influence the data flow. For example, an actor may be the sender of the data as part of their working role, e.g., a doctor's receptionist acting as a data processor in processing patient records, and at the same

time, a friend of one of the data subjects whose data they are processing. Each role in turn will have accepted, or implicit, norms and values that will need to be considered as part of any assessment. For instance, while it may be acceptable for the doctor's receptionist to share the data with the doctor or other health professional as part of their work function, it would not be appropriate for them to divulge any of the details in a social setting when, for example, the data subject and the data processor may attend a party socially. Thus, depending on the role will depend on how privacy is perceived and handled.

We contend that CI can be adapted to provide a *practical* mechanism for designing privacy into organisational decision-making when conducting privacy risk assessments for CPS. To illustrate how this can be achieved, we present the DPIA Data Wheel: a practical adaptation of how Privacy by Design (PbD) [15] can be incorporated into the decision-making process through Contextual Integrity.

3. The DPIA Framework

The DPIA Framework was created as part of a GDPR implementation study, conducted in collaboration with a local Charity in the UK [5]. One outcome of this study, was a data protection impact assessment, "the DPIA Data Wheel" (see Figure 2), devised to facilitate the charity's assessment of the privacy risks of their processing activities by including context as part of the design.

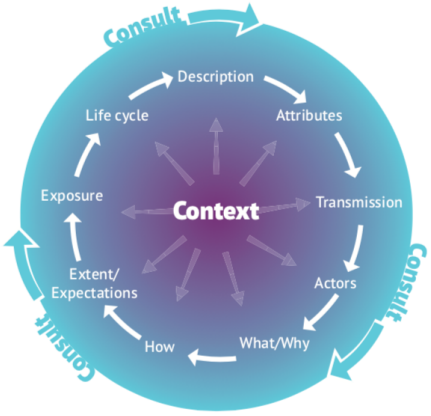

Figure 2. Data Protection Impact Assessment (DPIA) Data Wheel.

In creating the DPIA Data Wheel, we sought to integrate CI to GDPR obligations around DPIA and establish how CI could be incorporated into the DPIA process, using the concepts devised in a pilot study, ContextuaL Integrity for Open Data (CLIFOD) [16] (see Section 3.1). This was done through an analysis that sought to first, align the guidance provided by the Information Commissioners Office (ICO) in the UK around DPIAs [17] with GDPR and advice from the EU (see Section 3.2). This was then aligned to CI through CLIFOD (see Section 3.3) to create the final framework (see Section 4).

The DPIA Data Wheel was empirically evaluated as part of the Charity GDPR implementation study in three real-world settings. First, the DPIA framework was evaluated in an organisational setting, working in collaboration with management at a charitable organisation. The second evaluation involved consulting and collaborating with staff at the charity through a series of training workshops to further validate the framework. Third, the participation was widened to include peers by evaluating the DPIA framework in four seminars, held as part of a one-day workshop for a group of 40 charitable organisations based in the local area (see Section 5).

3.1. CLIFOD Pilot Study

To explain how the concepts within the DPIA Data Wheel were created, it is necessary to first explain how CI was translated into a practical risk assessment framework for supporting organisational decision-making around privacy. This process began with the creation of a meta-model of CI

(see Figure 3) that illustrates how CI can be translated and represented in a visual model that can be applied in practice [18].

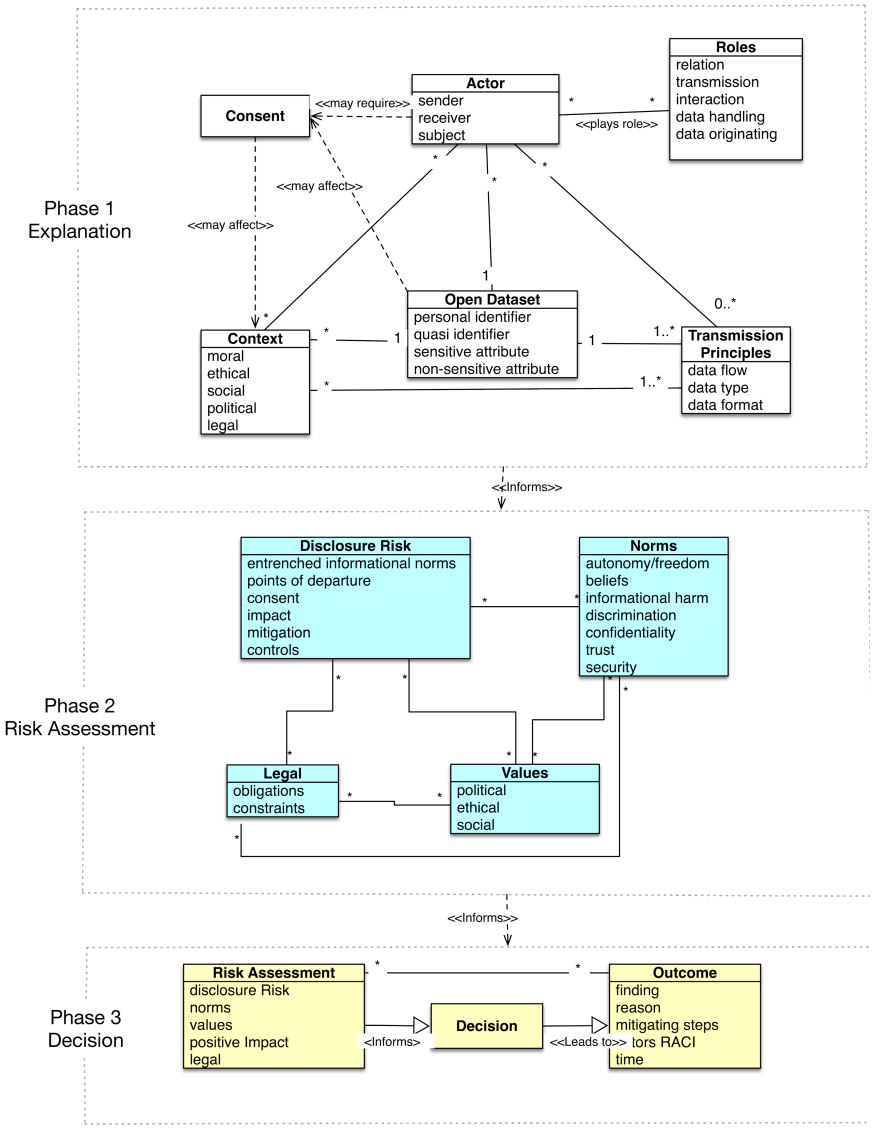

Figure 3. Meta-model of contextual integrity.

From this, we expanded on the idea of using CI to understand privacy risks by applying the concepts of CI to the decision-making process for open data publication in a pilot study, CLIFOD. In that work, the CI principles were used to create a privacy risk assessment questionnaire to aid decision makers in assessing the risks of making data available in open format [16].

The CLIFOD framework sought to incorporate the meta-model of CI into privacy risk assessment to facilitate informed decision-making for whether or not data can be published as open data. In creating CLIFOD, the two core elements of CI were used.

3.1.1. CI Core Elements Used in CLIFOD

1. *Three Overarching Phases*—the three key principles; "explanation, evaluation and prescription" [14] were translated into three distinct phases for framing the CLIFOD questionnaire. As part of this, the language used by Nissenbaum was translated to become;

    - Phase 1 became "explanation", which considers the existing practice, i.e., what the current (or proposed) context and processing practice(s) are;

- Phase 2 became "risk assessment"—this looks at the proposed change to the context and/or processing practice and what risks might be associated with these changes; and
- Phase 3 became "decision", which asks that the consequences or potential consequences (i.e., the outcome) of making the change be considered [16].

2. *Three Perspectives*—Beneath the first two phases, CLIFOD asks that privacy be considered from three perspectives;

- **"Actors"**—i.e., the data "subjects, senders and receivers", referring to the people who will be working with the data;
- **"Attributes"**—referring to the data elements which make up the dataset; and
- **"Transmission Principles"**—i.e., the data flows between actors.

3. *Nine Decision Heuristics*—Finally, to inform the questions within the questionnaire, the nine decision heuristics ([14], p. 181) were used to help formulate the individual questions.

3.2. Aligning GDPR and ICO Guidance

We used the concepts derived in the CLIFOD pilot study to incorporate CI into the DPIA process. However, the first step in creating an effective DPIA framework, was to ensure this would comply with GDPR obligations and guidance for conducting DPIAs. To this end, the guidance from the text of GDPR (Articles 5 & 35 and Recitals 90–94); the recommendations of Working Party 29 on DPIAs [19] (hereafter just referred to as *GDPR*), and the information Commissioner's Office (ICO), the governing authority for data protection in the UK [17], was used as the starting point.

This analysis began by looking at what the DPIA is actually seeking to accomplish, which is to support an effective, repeatable and detailed privacy assessment of data processing activities during its lifecycle with the organisation, and then how this could be adapted to fall into the CI phases devised in previous work *explanation, risk assessment and decision*, as described in Section 3.1.1 and [20].

To present this analysis, a logic model method was used. Research shows that modelling is an effective tool for communication of a cause of action, a programme or a process. For example, visualisation has been shown to help explain "how to get there" [21], and enhance understanding and communication, for example, of risks [22]. Therefore, a decision was made to depict the transition from the identified documentation in a visual manner. Therefore, a logic model was created to try to fit the process into some form of acronym or model that would provide a visual representation that practitioners could use for a quick overview.

Thus, starting with the nine steps outlined by the ICO for conducting a DPIA [17], these were mapped through a series of logic models to the six GDPR principles according to how they relate to each step. This is depicted in Figure 4, which shows the ICO principles in the first column, and then how these have been aligned to each of the GDPR principles in the second column.

3.3. Aligning CLIFOD to ICO Guidance and GDPR

Next, to incorporate CI, we used the outcomes from the CLIFOD pilot study as the basis for introducing context into the DPIA framework (see Section 3.1.1). To this end, work began on analysing how the CI principles used in CLIFOD could be mapped to the meta-model of Contextual Integrity in Figure 3 and aligned to the ICO DPIA Guidance and the GDPR Principles in Figure 4.

Figure 5 shows how the three phases of contextual integrity (CI) used in the meta-model and CLIFOD: *Explanation, Risk Assessment and Decision* (see Section 3.1) have been aligned first, to each of the ICO steps (column 2) and then, to the GDPR principles to which they relate (column 3).

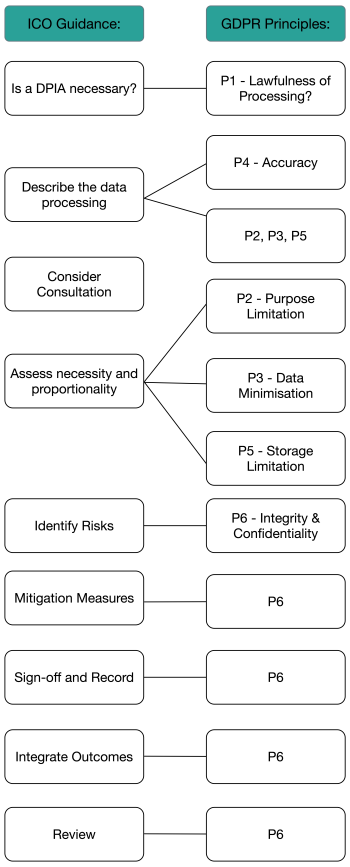

Figure 4. Aligning ICO DPIA Guidance to GDPR Principles.

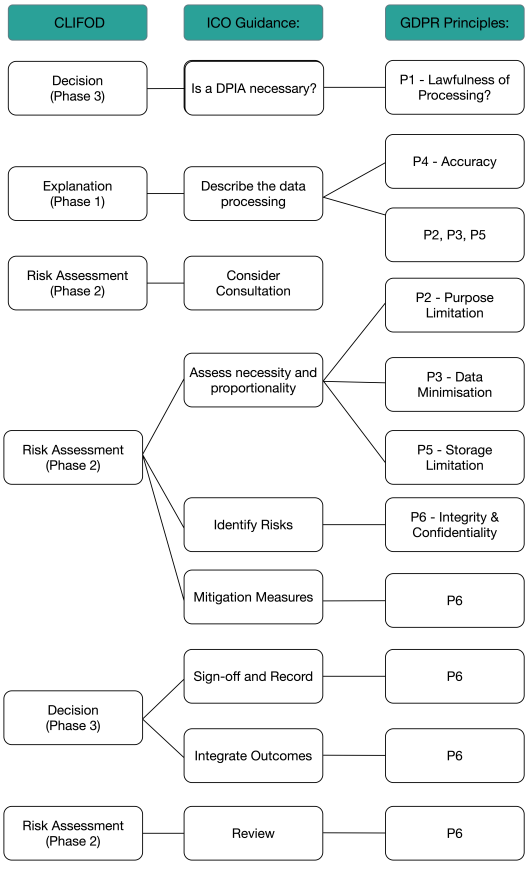

Figure 5. Aligning CLIFOD to ICO DPIA Guidance and GDPR.

4. The DPIA Data Wheel

At this stage, some of the concepts from ICO and GDPR were remodelled slightly in order to align the flow of CLIFOD with conducting a DPIA. Figure 6 denotes how the GDPR Principles were merged with and aligned to the three CLIFOD Phases (Column 1) before re-arranging the steps in CLIFOD to align with the flow of the ICO guidance (Column 2). Finally, in Column 3, the GDPR principles were used as the basis from which a series of questions could be created to flesh out the questionnaire itself and guide the practitioner through the process of how to conduct a DPIA. These questions were devised to incorporate all the aspects of CI to form the "Data Wheel" element of the framework.

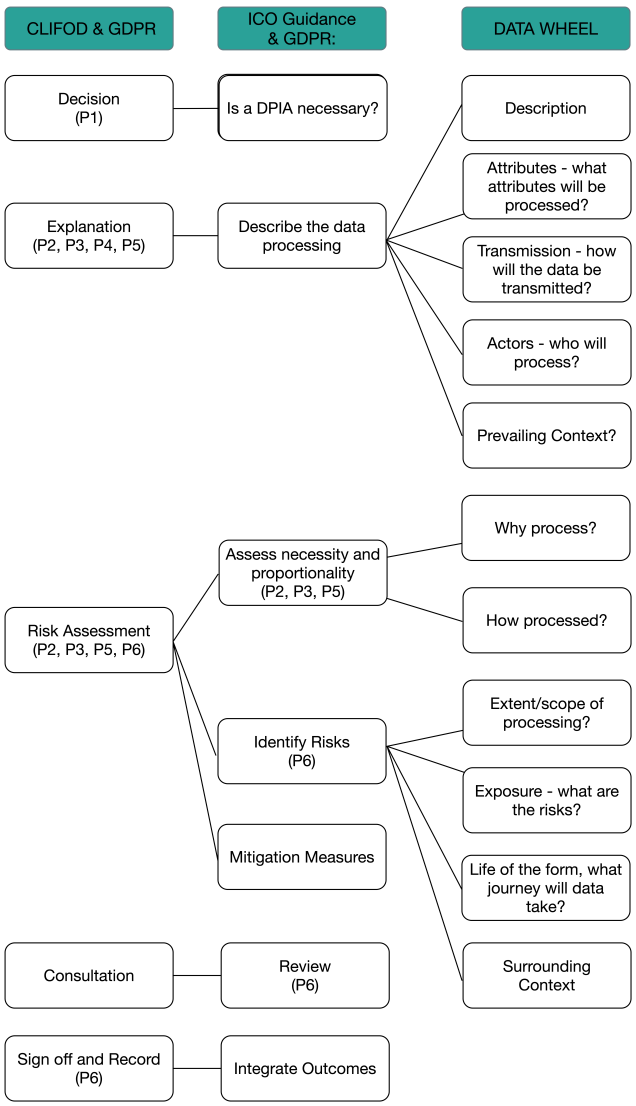

Figure 6. From CLIFOD to the Data Wheel.

4.1. The DPIA Data Wheel—Questionnaire

To create the questions themselves, the questions from CLIFOD were revisited to ascertain how these could be aligned with the GDPR principles and conducting a DPIA (see Section 4.2). However, because a DPIA is not always necessary (GDPR only requires a DPIA to be conducted for *"high risk"* processing activities (see Section 6.2), a pre-assessment questionnaire was added to the beginning of the Data Wheel to allow practitioner's the opportunity to decide whether a DPIA is necessary before completing the Data Wheel (see Figure 7).

This pre-assessment became the DPIA element of the final framework, a short questionnaire that decision makers can use for establishing whether or not the processing or proposed processing is likely to be classed as high risk; this is depicted in Figure 7.

DPIA Assessment for (name the system/process or process being asses				Date:
DPIA	**Need for a DPIA**	**QUESTION**	**ANSWER**	**Suggested outcome/Advice**
D	**DATA**	Will a new system, project or process be implemented that involves collecting, processing, transmitting, sharing and/or storing of data or are there any changes to an existing system, project or process?		
P	**PROCESSING**	Will the system, project or process involve any of the		DPIA required
I	**IMPACT**	Is the system, project or process likely to involve any of the following:		DPIA advisable
A	**ASSESSMENT**	Based on the answers above, DPIA required?		
		If decision is negative, please record the reasons for not carrying out a DPIA here:		

Figure 7. Need for a DPIA.

The answer column next to each question contains a drop-down list of where a DPIA is required (next to the *Processing (P)*) or advisable (next to the *Impact (I)*), these lists have been devised based on Articles 6 (*lawfulness of processing*) and 9 (*processing of special categories of data*) of GDPR, respectively.

4.2. The "Data Wheel"

Following the pre-assessment, if a DPIA assessment is deemed necessary, users will move on to complete the rest of the privacy risk assessment by completing the Data Wheel. The Data Wheel was created around Nissenbaum's three key elements, with the CLIFOD translation of the three phases ("explanation, risk assessment and decision" [16]) used to delineate the assessment and create three overarching phases for the Data Wheel assessment.

Figure 8 depicts the Data Wheel activity flow. The flow has been delineated using the three CLIFOD phases to guide which parts of the Data Wheel assessment fall under each phase as follows.

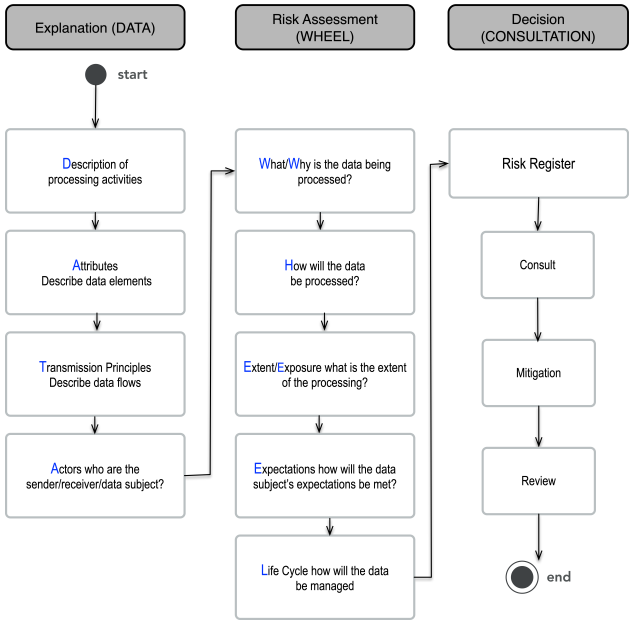

Figure 8. DPIA Data Wheel activity flow.

4.2.1. Explanation = Data

In the first phase, the explanation phase of CLIFOD has been translated into the "Data" part of the Data Wheel. Here, the initial letters of the word Data have been used to establish the background or explanation for what is being assessed. Thus, the questions here have been devised to guide users to gather information about the project, system or processing activity being undertaken as well as details about the data, the actors and transmission principles. An excerpt of this can be found in Figure 9. As part of this, users are asked to complete a data register to identify the individual data elements (see Section 4.3). In addition, questions are asked to help establish the prevailing context of the processing activity. For example, if a DPIA assessment is conducted on an existing processing activity due to be altered was the data collected with a view to process beyond its original purpose, and if not, was consent for further processing obtained from the data subject?

DPIA DataWheel		QUESTIONS	Answers:	DPIA Review - answers (if different from original)
D	Description	What is the purpose of the data collection/processing?		
		What is the system, process, project or dataset about (subject matter/context)?		
		What is the lawful basis for processing the data?		
		If special category data processed, please also provide secondary lawful basis for processing the data		
A	Attributes	Attributes - please describe what data will/has be/been collected?		
		What attribute types will be included: PI, QI, Sensitive, non-sensitive? (attributes/dataset) - please select all that apply. *If this is a new project or system, please also complete the Data Register tab with details of each attribute.*		
T	Transmission principles/ Information Flows	How will the data be processed internally within the organisation?		
		Locate applicable entrenched informational norms and identify significant points of departure. Consider legal and ethical obligations e.g. consent, is it required/will it be obtained?		
		Will the data be transmitted to external stakeholders? (transmission principles)		
		Please describe the information flows with external stakeholders		
A	Actors	**Actors - Internal** **please note who is the data processor(s), data controller, data subject, other internal stakeholders who will use/access the data and what their role is within the organisation**		
		Please confirm who is the data controller		
		Responsible Person - name and contact details of the designated Data Controller(s)		
		Data Owner (if different from Controller)		

Figure 9. Extract of "DATA" Wheel.

4.2.2. Risk Assessment = Wheel

The "Wheel" element of the Data Wheel (see Figure 10) corresponds to the risk assessment part of CLIFOD (Phase 2). This, therefore, asks questions to help decisions makers identify what privacy risks might be associated with the proposed processing activity or, if assessing changes to existing processes, the actual processing activities. Moreover, in identifying the risks, the wheel asks users to score and specify for each risk, how this relates to (a) the data subject and (b) the organisation. To further aid this, users are encouraged to also complete the journey the data is likely to go on as part of its life cycle by completing the life of the form supporting questionnaire (see Section 4.3 and [5] for more details).

To cover context, at the end of the 'Wheel' section within the framework, a number of specific questions within the Wheel that pertain to the specific contextual enquiry areas that need consideration according to Nissenbaum, namely any threats to or potential harm to the data subject that could arise from an infringement of political, social or moral values; legal obligations; loss of autonomy

or freedoms; discrimination; power imbalance or the affordance of prerogatives or privileges [14] have been devised. These correspond with the contextual questions, devised for the CLIFOD questionnaire (https://figshare.com/articles/Contextual_Integrity_Privacy_Risk_Questionnaire/12220334).

DPIA DataWheel		QUESTIONS	Answers:	Review - answers (if different from original)
W	What /Why	What are the benefits of the processing for the data subject?		
		What is/are the desired effects of the processing for the data subject?		
		What is the desire effect of the processing for the organisation?		
		What is the primary legal basis for collecting/processing or handling the data?		
		If applicable, what is the secondary legal basis for collecting/processing or handling the data?		
		What are the benefits of the data processing for you (the organisation)?		
		What are/is the desired effects of the processing for the organisation?		
		Why is the data being collected/processed? (purpose limitation/relevance)		
H	How	How much data will be collected?		
		Who is responsible for security around manual data handling, processing or storing		
		How will the data be collected?		
		How is/will the data be accessed and used/processed?		
E	Extent	What is the extent of the processing - will we require consent? (lawful processing, transparency)		
		Identify any risks of the dataset or individual attributes, being obtained or accessed by unauthorised parties or means in such a way that they can pose a risk a data subject? (please be specific as to what risk and how this might pose a new risk)		
		Security - how is/will the data be protected and kept safe?		
	Exposure	Who is responsible for access control and data security (electronic data handling, processing or storing)?		
		What are the risks of the dataset or attributes, being linked to external data in such a way that they can pose a risk of contributing to re-identification of a data subject? (please be specific as to what risk and how this might pose a new risk)		
		How will data handling boundaries be set, measured and controlled?		
E	Expectations	How is/will compliance be measured and controlled?		
		Data subject right to access and erasure requests, how is/will this be managed/accommodated?		
		How is/will compliance be evidenced?		
		How will we meet stakeholders expectations and adhere to data subjects rights?		
L	Life cycle	What is the expected data life cycle? i.e. for how long will the data be 'live' and processed		
		Has data limitation been considered, is all the data being collected necessary?		
		How is/will the data be stored?		
	Life of the form	Life of the form - what journey(s) will the data take as part of it's lifecycle?		
		How do/will you delete the data?		
		How long will the data be kept?		

Figure 10. Excerpt of Data "WHEEL".

4.2.3. Decision = Consultation

The third and final phase of CLIFOD, decision, becomes the consultation in the Data Wheel. This phase involves reviewing the risks by consulting with stakeholders and identifying suitable mitigation strategies for each risk identified. This phase in the Data Wheel also includes a review element to depict that the DPIA Data Wheel is a living document or assessment, that will need reviewing on a regular basis.

Within each of the first two phases of the Data Wheel, questions are then asked to guide decision makers through the DPIA, the questions concerning procedure such as, how long the data will be retained for, and whether consent has been obtained from the data subject, have been devised based on GDPR and guidance mentioned above.

4.3. Supporting Questionnaires

In completing the Data Wheel, some aspects required a more in-depth analysis and consideration. To this end, two of the forms created as part of the GDPR Implementation case study [5]

Data Register a spreadsheet devised to capture details about each data attribute (individual data item) processed by the organisation. This includes gathering all legally obligatory details pertaining to the data required under GDPR Article 30. For example, it asks that data processing is justified and each attribute is categorised according to data sensitivity;

Life of the Form a spreadsheet designed to capture the "life of the form", i.e., the journey the data goes on as part of its lifecycle within the Charity. The life of the form spreadsheet captures details of the journey the data is likely to take during its lifetime with the organisation, allowing for up to 10 'journeys' (see Figure 11 for excerpt).

The intention in including these forms was that decision makers can use the information gathered here to inform the privacy risk assessment. These forms were deliberately devised to capture a high level of detail. The intention being this would help stimulate discussion and encourage wider consideration around privacy risk, and the context within which data is used being taken into account as part of the assessment. This ensures the resulting privacy risk register is fully informed, thorough and comprehensive.

Form/data Name **Question**
Birth (where was the form/data born? why is the data being collected?)
Intended uses: What is the form/data intended for? What is the purpose of the data collection?
Actual uses: What is the form/data actually used for?
Regularity: How often is the form/data used?
Who: Who fills in the form/data? Who collects the data?
When: In what circumstances is the form/data filled in or collected?
Why: Why is the form/data filled in?
Format: What format is the form/data in (e.g. manual paper based or electronic)
Home: Where is the form kept or stored (where does the form live)?
does it get moved from it's home (if yes, then then back to the journey)?
Storage Format: In what format is it kept or stored?
Access: Who can access the form once it is stored?
Retention: How long is the form stored for?
Disposal: How does the form get disposed of?
Journey 1: **This is intended to capture the data journey i.e. whenever the data travels, who it is shared with, how it is shared (faxed, emailed, verbal etc.) and how often this happens.** **To this end the questions that follow are cyclical and apply every time the form/data (and therefore, the data, travels). Please complete the questions for each journey that form/data takes whether that is physical as in the paper being moved, electronic as in the data being shared either by scanning,**

Figure 11. Excerpt—Life of the Form Spreadsheet.

4.4. Consultation

The DPIA Data Wheel facilitates the gathering of comprehensive background information about the data, the actors and the transmission principles to inform the risk assessment in the Data Wheel.

For the consultation element, this has been "removed" from the process and instead used as a *loop* circumscribing the DPIA Data Wheel (see Figure 2) to show that this element is a continuous and ongoing process. The idea behind consultation is to ensure all relevant stakeholders who have an input or interest into the process, system or project have an opportunity to help identify potential privacy risks and be consulted about such risks, so they too can take part in devising the mitigation strategies.

Thus, the final privacy risk assessment framework created can be used to assess the implications of data processing for both the organisation and the service recipients (*the data subjects*) and therefore, arguably, this framework can be used as both a PIA and a DPIA assessment. This combines any privacy risk decision making an organisation needs to make into one holistic framework, the DPIA Data Wheel.

5. Evaluating the DPIA Data Wheel

The GDPR implementation study was used as the vehicle for evaluating the DPIA Data Wheel [5]. This study was conducted as a Case Study following Yin's methodology on Case Study research [23]. The protocol for this case study can be found at: https://figshare.com/articles/GDPR_Implementation_Case_Study_Protocol/12220250.

The evaluation of the DPIA Data Wheel was carried out over a three-month period. As part of this process, the DPIA Data Wheel was subject to three empirical evaluations as follows:

1. Evaluation One: Assessment of the DPIA questions (by three: Practitioners; Academics; and Peers)
2. Evaluation Two: Initial completion of the DPIA Data Wheel and Staff consultation, consisting of three training sessions attended by 29 staff;
3. Evaluation Three: Peer Consultation, consisting of a workshop and four seminar groups, attended by 40 charity sector employees.

5.1. Evaluation One

In the first evaluation, three groups of assessors were approached and asked to comment on the format, layout and the questions devised for the DPIA Data Wheel framework. These groups were:

Academic three Academics, two who specialise in Security, HCI, CPSs and privacy and one with a process and methodology background;
Practitioners three practitioners with a background in security and/or data management;
Peers three peers (PhD students with expertise in risk and/or security) were approached for comment.

Each assessor provided valuable feedback resulting in revisiting and revising some of the questions. This included adding a glossary and amalgamating the instructions for each worksheet within the prototype spreadsheet into an introductory worksheet containing instruction for how to work through the framework, and details about what each worksheet covers.

In total, seven evaluations and consultation sessions were conducted. These were attended by 69 participants who between them identified a total of 88 different privacy risks. At the end of Evaluations Two and Three, both participants and facilitators were asked to complete a post-training questionnaire (this can be found in the case study protocol, Appendix I and J respectively (see Section 5 for link).

5.2. Evaluation Two

Evaluation two began with the DPIA Data Wheel being completed and evaluated by Management at the charity. Two Managers, the Chief Financial Officer (CFO) and one of the Directors, collaborated to complete all the elements of the DPIA framework for six different forms used within the organisation, with each form corresponding to a data handling process in regular use within the organisation. This resulted in a number of privacy risks being identified for each process. For example, the completed

DPIA Data Wheel for the client care plan, one of the most frequently used forms within the organisation, resulted in 17 risks being identified, mostly related to unauthorised access to data or loss of data as a result of external interference or influences of some description.

The data captured on the data registers for each of these was transferred onto the Master Data Register. This aided the DPIA assessment itself, and helped the charity keep their data register up to date, thereby demonstrating compliance to the UK Information Commissioner's Office (ICO).

Based on the completed DPIA assessments from Management, a decision was then made to use the client care plan as the basis for consultation as part of the staff training session. Research suggests that incorporating known scenarios into the teaching materials leads participants (in this case, staff) to better, more lasting outcomes. This means they are more likely to apply their learning in practice [24]. This, therefore, influenced the decision to use this DPIA. However, the main reasons for choosing to use this DPIA assessment were; first, the care plan contains a lot of very personal and highly sensitive information that requires safeguarding under GDPR. Second, the charity was in the throes of changing how the care plan is completed and used in practice from a manual handling process to electronic recording and processing in future. This change would introduce an automated element to the charity's data processing whereby any updates made by staff on their smart devices (phone and/or iPads) would interact and update via the organisation network to automatically update and synchronise with the rest of the connected devices and the cloud. This meant that the data transmission principles would need to change as a result. Third, using a process that staff were very familiar with meant they would have practical experience of how the form is handled, as part of the daily routine within the organisation, and therefore, a good idea about what sort of risks might be associated with this handling of the form.

The next stage of this evaluation consisted of the staff training sessions, used the pre-completed manual process form for the care plan. This evaluation consisted of a training session on the changes introduced by GDPR and the DPIA, before moving on to the evaluation of the DPIA. As part of this evaluation, staff were provided with a handout (a copy of this can be found in the case study protocol, Appendix H (see Section 5 for link) containing information about GDPR, how this affects them and their work with data and the pre-completed DPIA Data Wheel.

The staff training sessions were attended by 29 members of staff. Of these participants, 22 considered themselves to have limited understanding of GDPR, and most claimed to have little knowledge about DPIAs prior to attending the training. However, after the session, 21 felt very or reasonably confident in attempting to conduct a DPIA for themselves going forward. Across all sessions, 36 privacy risks were elicited with potential mitigation strategies identified for each. This not only provided staff an opportunity to consider the risks of how they handle data as part of their work activities, they also identified solutions for overcoming some of the obstacles identified themselves. We believe this makes it more likely they will implement the required data handling mitigations in future [24,25].

5.3. Evaluation Three

The third evaluation took place as part of a one-day workshop where 40 participants were invited to attend from all the local charitable organisations in the area. The format of the workshop was to inform local charities of the changes brought in by GDPR and to help them demystify the DPIA process and give them confidence in conducting DPIAs in practice. To this end, as part of the workshop, participants were divided into four seminar groups for a practical run-through of completing a DPIA.

For these seminar sessions, we used the same DPIA Data Wheel assessment that had been pre-completed by the charity's management in the second evaluation as the basis for the simulations. However, participants were asked to consider how the proposed change from manual to CPS processing might affect the privacy of the individuals involved.

The seminar groups were facilitated by individuals with experience and backgrounds in data management and security. The facilitators were instructed to facilitate rather than steer the privacy

risk discussion to avoid bias being introduced into the evaluation or resulting privacy risk register (a copy of this can be found in the case study protocol, Appendix H (see Section 5 for link).

The format of the session was designed so that participants would first, review the Data Wheel answers provided by the management team. Second, discuss what the potential risks might be associated with the change in data transmission principles from manual to CPS, with the session facilitators noting these on the privacy risk register within the framework. Seminar participants were provided with handouts providing details of GDPR and a copy of the pre-completed Data Wheel (as used for the staff training).

Thus, these seminar sessions were used as an opportunity to; (i) further evaluate the DPIA Data Wheel; (ii) widen the DPIA consultation to an extended peer group within the charity sector, thereby getting a broader perspective on potential privacy risks; and (iii) use this and the training sessions as an opportunity to conduct two DPIA risk assessments on the client care plan, one for the existing manual process and one for the proposed new process.

5.4. Evaluation Results

Most participants in Evaluation Three did not consider themselves security or privacy experts, with just over half reporting that they considered themselves to have some prior knowledge of GDPR. Similarly, most participants stated they had little or no prior knowledge or understanding of DPIAs prior to attending the workshop. Following the workshop, when asked how likely they were to use the learning from the workshop and seminar in their daily work in future, just over half of the participants reported that they were extremely or very likely to apply what they had learnt in practice.

6. Related Work

6.1. Organisational Decision Making and Privacy Risk

The idea of adopting a risk-based approach to decision-making is widely accepted around the world, for example, [26–28]. Risk assessment can be applied to any area including; financial risks [29]; project risks [30]; and safety and security risks of CPS [13]. Indeed, any aspect of organisational decision-making can be informed by a risk assessment [31]. Applying this to CPSs, a large number of challenges exists including how to design and maintain security of such systems [11].

Several risk frameworks provide direction on making decisions concerning privacy risk, e.g., [32,33]. For more specific areas such as software design, a variety of privacy requirements frameworks exist that decision makers can utilise to assess the privacy implications [34]. For example, the PriS framework has been devised to help software designers elicit privacy requirements [35], while LINDDUN helps users assess privacy threats by modelling data flows to facilitate identifying what privacy enhancing technologies (PETs) can be applied in system design [36].

For more general privacy risk assessments, a popular privacy risk assessment framework is the Privacy Impact Assessment (PIA) [37]. This seeks to provide a common methodology for assessing what privacy impacts might result from a system, product, service or other activity in order that appropriate mitigation strategies can be put in place [38]. Further, conducting a PIA is a recommended method for conducting privacy risk assessment and incorporating PbD [15] into organisational practice in many countries including Canada, the US, Australia and the UK [37,39].

These privacy frameworks do, however, suffer from three limitations. First, they fail to account for the wider human context within which such systems might be used or interacted with. Second, the perspective from which all of these methods ask that privacy is considered is from the organisational viewpoint, for example, to help them identify the best methods of securing the system, process and/or data; they do not consider the risks to the data subject, which is what assessing privacy risk under GDPR requires. Third, whether or not privacy risk is assessed is dependent on the organisation and their policy, which may not prescribe that privacy assessment must be conducted as standard.

6.2. Mandatory Privacy Risk Assessment

The introduction of GDPR changed this landscape by making privacy risk assessments compulsory for any organisation that processes data pertaining to any EU citizens [12]. One of these new obligations is a requirement to conduct a DPIA for any *"high risk"* data processing activities (Article 35, GDPR).

This means that although many organisations may already conduct privacy risk assessments or PIAs as standard, the DPIA introduces some notable changes. First, the perspective from which privacy risk must be assessed has been shifted. According to GDPR, in conducting DPIAs, organisations are asked to assess risks from the perspective of the data subject, rather than from the perspective of the organisation, as is traditionally how business assesses risk. This requires that the likely privacy risks to the data subject, are considered and what consequences, or likely impact, a potential data breach might have on the individual. This means that organisations should first consider how the processing might affect the individual, before identifying appropriate safeguards around the data, the system or the processes within the organisation. Second, conducting a PIA is voluntary in most jurisdictions, meaning an organisation may not include PIAs as part of their risk analysis process [38], whereas the DPIA is now an obligation rather than a recommendation [12].

6.3. Contextual Integrity and Privacy Risk

Westin first observed that privacy is context dependent by making a distinction between privacy as autonomy or dignity, and the right to control personal information [40]. Subsequent work has considered the context of data privacy by dividing privacy into different spheres [41], identifying that boundaries exist between different aspects of privacy [42], and discussing how to ensure context is included as part of the consideration in making decisions around privacy, in particular, data privacy [14].

In considering privacy risks in relation to personal information, Nissenbaum asserts that data privacy refers to "a right to an appropriate flow of information" [14]. To achieve this, Bamberger et al. [43] contends that organisations must integrate context into their corporate structures, values and decision-making processes. We assert that, for context to be fully considered, this integration must include consideration of how privacy will influence and be affected when CPS structures and processes utilise and process data.

6.4. Previous Applications of CI

There are several examples for how the CI framework might be applied in practice. For example, CI has been used to inform privacy best practice in access control policies [44,45], understand information flows [46], determine levels of privacy protection in social networks [47], cloud storage environments [48], and support virtual message exchange [49]. These examples demonstrate how, in theory, CI may be applied in different scenarios, discussing how CI might work in the given project or situation. However, these studies do not practically apply CI to real data, thus failing to demonstrate that CI works in practice.

Several recent studies have tried to address this gap by applying CI to real data. For example, CI has been used to establish user expectations and accepted norms in sharing location data [50] and evaluate context-aware app privacy control settings [51]. However, these studies use CI to assess user perceptions or tolerances; they do not consider how CI might be used to assess privacy risk of CPS or apply privacy design principles into CPS by default.

6.5. GDPR and Context

Similarly, GDPR also requires that privacy risk must be considered *in context* as part of the requirement to assess privacy risk. This, according to Recital 76, requires practitioners to take into account the "nature, scope, context and purposes" of how the data is used (*processed*) [6]. This word,

context, is mentioned a total of 57 times, on 50 separate pages, within the text of the GDPR, yet, nowhere does it clarify, or explain, exactly what that means in practice. We believe that CI provides an effective mechanism for incorporating context into the privacy risk assessment process.

This problem of lack of clarification is also evident with existing privacy risk assessment guidance documents. For example, if we look at the direction and advice provided in the risk frameworks [32,33] and the PIA guidance for conducting privacy risk assessments [39], most of these documents mention context only in passing. Thus, while they may ask users to consider context as part of the guidance, they fail to elaborate or explain how this might be achieved. As a result, the PIA process often lacks proper structure and little detailed guidance is available for how to conduct PIAs [38]. Furthermore, where the PIA historically asked that privacy risks to the organisation and its systems be assessed, the DPIA requires that privacy risks to the individual (the data subject) are to be assessed, thereby changing the perspective from which such assessments are to be conducted.

The DPIA Data Wheel provides a repeatable, holistic privacy risk assessment, that we believe can support consistent privacy risk assessment for CPS processes and systems. This will allow organisations who operate CPS to conduct both PIAs and DPIAs in one framework and identify suitable mitigations for each risk identified as part of the assessment. This, in turn, will allow these organisations to not only meet their obligations under GDPR (Article 35, GDPR), but also facilitate assessing privacy risks to the organisation through one holistic privacy risk assessment.

7. Discussion

7.1. Individual vs. Organisational Risks

The different perspective from which privacy risks need to be assessed when conducting DPIAs appeared to be a greater challenge than originally anticipated. Both the workshop and staff training sessions were preceded by explanatory sessions and talks about GPDR and DPIAs, which made it clear that, in conducting a DPIA, the desired outcome was to identify privacy risks to both the data subject and to the organisation. Yet, despite this, as part of the evaluation, the participants identified only risks to the organisation. There were no risks to the individual included at all from any of the sessions.

This lack of individual risks clearly showed that the research team underestimated the effect of changing perspectives and how difficult this would be for practitioners to appreciate. The fact that mandatory privacy risk assessment requires privacy risk being assessed from the perspective of the individual (see Section 6.2) appeared to be more difficult to comprehend for the practitioners than originally envisaged. This became quite clear as throughout the evaluations of the DPIA Data Wheel where, although participants identified many appropriate risks, most of these related to the organisation and/or the industry sector (charities), rather than the individuals whose data was being processed. This indicates either the distinction between the two different perspectives (data subject vs. organisation) was not highlighted sufficiently or, perhaps participants were so pre-conditioned to assess risks from an organisational perspective, that they failed to recognise or fully appreciate the difference. Future work will look at this to establish how best to address and overcome this issue.

7.2. Using Context for Discovery

The idea of having a distinct context section that contained specific guided questions around the values and norms that need to be considered as part of contextual inquiry within the Wheel (see Section 4.2.2), provided a very useful aid for guiding the discussion; this helped participants apply contextual inquiry in practice. However, to fully appreciate and get the most from the practical application of context, more in-depth explanation of these concepts as part of the consultation process in any future applications of the framework, will help raise awareness of contextual inquiry, and how to consider context. This will help identify more privacy risks and suitable mitigation strategies.

7.3. Context as a Form of Provocation

When completing the supporting questionnaires during Evaluation Two, the most varied and vibrant area for discussion about risks was the context sections. The questions prompted the management to think about how the actions of staff might be perceived by service recipients. Thus, when they were asked probing questions about the prevailing and surrounding context of how staff and volunteers handle (*process*) the data and how this might be perceived by service recipients or other stakeholders, the discussion became interesting. Initially, for the prevailing context questions, this did not seem to raise too many concerns. For example, in regards to discrimination, one of the areas identified as one of the four challenges by Wachter [4], staff felt that potential discrimination was unlikely as this was an area staff and volunteers received a lot of guidance and training on. This would indicate that, at least for some areas, the charity has ensured sufficient training and awareness is raised among staff to safeguard service recipients from harm involving potential discrimination. Nonetheless, the assessment did raise concerns that had not been previously considered by management.

Context was used in a similar manner in Evaluation Three. Interestingly, in these sessions, no changes had been recorded in the context sections for any of the groups. This could have been due to lack of understanding on the part of the participants and/or facilitators. This was highlighted by one of the facilitators as part of their feedback where they stated: *"I don't think the instructions were lacking it was more my lack of experience with facilitating that may have impeded the process"* (F2). Further, the facilitators had been specifically instructed not to 'direct or lead' the discussion, rather, let the participants discuss the answers among themselves. This, in hindsight, might have been a mistake as a more in-depth discussion of context could have provided some insight and understanding of how context affects data flow, thereby helping participants appreciate the wider implications of assessing privacy risks. A similar sentiment was provided in the evaluation feedback provided by participants, with one attendee commenting: *"Some areas seem grey and it is so individual to each charity it seems a minefield"* (A17).

7.4. Using Context to Identify Data Handling Power Asymmetries

When the questions in the surrounding context section required participants to consider whether data handling might pose a power imbalance or threat to the freedom of the data subject, a few concerns were highlighted as a result of the prompts provided by the questions. For example, service recipients in active treatment reside on the premises of the charity. While service recipients' are in residence, staff have the power to ask service recipients to leave if they endanger other service recipients or break "house rules". This could be perceived by service recipients as an abuse of power in that they would have to leave the house. One potential consequence of this would be the cessation of treatment, which in turn would increase the risk of a relapse into addiction. The risk of this occurring was rated as low but the impact on the individual would, however, be significant in view that a relapse could potentially endanger the client's life.

After the assessment, the findings were presented and discussed with the management team who explained that all service recipients are informed of these rules. They were then asked to sign to signify they understand and agree them, prior to moving into one of the houses. However, the management team conceded that a suitable mitigation strategy of more staff training on how to avoid potential abuse of power situations might be appropriate. This was noted on the DPIA form, and signposted for being action by management.

7.5. Role-Specific Privacy Risks

During Evaluation Two, the risks identified by staff were all different from the risks identified by managers. Where management had focused on risks originating from external parties gaining access to data, staff viewed most risks as originating from internal threat actors such as service recipients seeing or gaining access to information they should not be privy to or staff errors resulting in potential

data leakage. The aspects around context were not really discussed beyond the answers provided by management initially. This was partly due to time constraints and partly, due to staff not feeling they could add anything to the list of risks already identified by the management team.

7.6. Generic and Specific Privacy Risks

In the seminar sessions in Evaluation Three, each seminar group elicited a different set of risks, ranging from generic risk, for example, *"loss of data"*, to much more detailed risks such as; *"Disgruntled employee may deliberately leak information and then report the leak to the ICO"* being identified. Similarly, in discussing potential mitigation strategies, the seminar groups who came up with generic risks also identified generic mitigation strategies, for example, *"back up data"*, whereas the group with the more detailed risks also produced more detailed mitigation strategies, for example, *"Ensure staff sign confidentiality agreement, staff training, criminal liability—appropriate staff contract, DBS check all staff. Access control on different types of data. Make everyone accountable"*.

Although participants were randomly selected for each of the groups, some would have more experience of risk assessment than others. According to the facilitators feedback, some of the participants had *significant* risk knowledge and understanding, although this was thought to relate more to security risk rather than privacy risk. Therefore, these disparities between the level of detail could perhaps be attributed to the level of expertise within each seminar group. The seminar sessions still proved useful in identifying and examining how changes in transmission principles would change the risks to the organisation, and what mitigations might help prevent those risks occurring.

8. Conclusions

In this paper, we presented the DPIA Data Wheel: an empirically evaluated DPIA framework. The DPIA Data Wheel exemplifies how PbD can be achieved through designing CI into the DPIA process. The framework was devised to provide a useful tool that decision makers can use to ensure contextual considerations are included as part of their privacy risk assessment process.

The DPIA Data Wheel framework was designed with charities in mind. However, it can equally be applied and used in any organisation who are required to conduct privacy risk assessments and/or DPIAs. This DPIA Data Wheel provides an exemplar, GDPR compliant DPIA process that incorporated two prototype spreadsheets (a Data Register and the life of the form, devised to capture details of the data flow within the organisation) from the GDPR implementation case study (see [5]). These prototypes have been included in the DPIA Data Wheel to facilitate organisations being able to collate appropriate evidence for demonstrating compliance with GDPR. For context, the DPIA framework questions integrated most of the questions from CLIFOD, including all the contextual questions, into the framework. Finally, the DPIA framework also incorporated a privacy risk assessment, and recording of suitable mitigation strategies to address any privacy risks identified, designed to aid practitioners in determining what privacy risks might be associated with data processing associated with the implementation of a new system, project or process or other data processing activity associated with CPS (see Section 3).

The DPIA framework presented in this paper provides decision makers with an exemplar for conducting a combined DPIA and PIA assessment in practice based on CI. Moreover, this DPIA framework not only helps decision makers conduct consistent and repeatable privacy risk assessments, it also guides them towards making informed decisions about privacy risks and provide them with demonstrable evidence of GDPR compliant processes and practices. This, we contend, is particularly useful in scenarios where boundaries between different processes or systems are blurred, such as CPS.

Some of the outcomes from the evaluations in Section 5 should not be entirely surprising. Historically, risk assessment is invariably concerned with what the consequences and likelihood of the risk occurring would be for the business and how this might negatively affect the organisation, rather than how they might affect the individual. Thus, decisions makers might be pre-conditioned into thinking about risks in terms of organisational risks. Therefore, asking them to now look at risk

from the perspective of the individual without first providing more direction and guidance is unlikely to result in the desired DPIA assessments Data Protection Regulation Authorities might hope for.

Our work demonstrates that the wider the consultation on the DPIA risks identified, the more in-depth and complete the resulting privacy risk register is likely to be. Moreover, in terms of context, what our evaluation illustrates is that, the more stakeholders are consulted, the more context is likely to be included in the assessment. This shows the importance of allowing each stakeholder group to add their different perspectives, thereby broadening the context being considered. Stakeholder consultation is also an opportunity for reciprocal learning, making participants more likely to implement and use the lessons learnt which, in turn, reduces the likelihood of the risks identified occurring.

While the breadth of the evaluation, and therefore the consultation, was inclusive and comprehensive, more emphasis needs to be placed on the procedure for conducting the DPIA and how to contextualise and relate the risks to the individual rather than the organisation to ensure wide stakeholder engagement. To address this, consideration needs to be given to whether and how the questions can be adapted to encourage a change in perspective, or illustrative examples can be incorporated into the framework questions.

To ensure the decision makers understand the distinction between risks to the individual and risks to the organisation, more emphasis also needs to be placed on making sure the underlying principles are fully understood by participants when conducting training or consultation on DPIAs. This can be addressed by incorporating more direction about context, and how it can be considered as part of the evaluation. One way this can be achieved would be to provide some worked examples as part of the learning material or, as mentioned above, as part of the instructions provided with the framework.

Future work will examine how more guidance and worked examples can be provided in future iterations of the DPIA Data Wheel and associated documentation. It will also look at how the DPIA Data Wheel can be applied to the design of CPSs, and used more effectively to provide better directed education and training. This will allow users to assess risks to the individual, before using these to direct how they can implement effective safeguards and practices around their personal data processing activities in future.

Author Contributions: Conceptualization, J.H.-B. and S.F.; methodology, J.H.-B. and S.J.; validation, J.H.-B., S.J. and S.F.; formal analysis, J.H.-B.; investigation, J.H.-B.; resources, J.H.-B and S.F.; data curation, J.H.-B; writing–original draft preparation, J.H-B.; writing–review and editing, J.H.-B., S.J. and S.F.; visualization, J.H-B.; supervision, S.F. and S.J.; project administration, J.H-B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lee, E.A. Cyber Physical Systems: Design Challenges. In Proceedings of the 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008; pp. 363–369. [CrossRef]
2. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
3. Giraldo, J.; Sarkar, E.; Cardenas, A.A.; Maniatakos, M.; Kantarcioglu, M. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Des. Test* **2017**, *34*, 7–17. [CrossRef]
4. Wachter, S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Comput. Law Secur. Rev. Int. J. Technol. Law Pract.* **2018**, *34*, 436–449. [CrossRef]
5. Henriksen-Bulmer, J.; Faily, S.; Jeary, S. Implementing GDPR in the Charity Sector: A Case Study. In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, 20–24 August 2018, Revised Selected Papers*; Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., Krenn, S., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 173–188. [CrossRef]

6. European Parliament and the Council of Europe. *General Data Protection Regulation (GDPR)*; Legislation REGULATION (EU) 2016/679; European Parliament and the Council of Europe: Brussels, Belgium, 2018.
7. Ebersold, K.; Glass, R. The Internet of The Internet of Things: A Cause for Ethical Concern. *Issues Inf. Syst.* **2016**, *17*, 145–151.
8. Ackoff, R. From data to wisdom. *J. Appl. Syst. Anal.* **1989**, *16*, 3–9.
9. Gausden, G. Privacy concerns as energy companies could be given access to all smart meter data and take readings every 30 minutes. *This is Money*, 10 May 2019; online.
10. EE Times. Benetton backs off RFID deployment. *EE Timmes*, 5 April 2003; online.
11. Ashibani, Y.; H.Mahmoud, Q. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
12. European Commission. *A New Era for Data Protection in the EU: What Changes after May 2018*; European Commission: Brussels, Belgium, 2018.
13. Lyu, X.; Ding, Y.; Yang, S. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 221–232. [CrossRef]
14. Nissenbaum, H.F. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*; Stanford Law Books: Stanford, CA, USA, 2010.
15. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*; Technical Report; Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2011.
16. Henriksen-Bulmer, J.; Faily, S. Applying Contextual Integrity to Open Data Publishing. In Proceedings of the 31st British HCI Group Annual Conference on People and Computers: Digital Make Believe, Sunderland, UK, 3–6 July 2017.
17. ICO. *Data Protection Impact Assessments*; ICO: London, UK, 2018.
18. Henriksen-Bulmer, J.; Faily, S.; Jeary, S. Privacy Risk Assessment in Context: A Meta-Model based on Contextual Integrity. *Comput. Secur.* **2019**, 270–283. [CrossRef]
19. Article 29 Data Protection Working Party. In *Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679*; Technical Report; The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data: Brussels, Belgium, 2017.
20. Henriksen-Bulmer, J.; Faily, S.; Katos, V. Translating Contextual Integrity into Practice using CLIFOD. In Proceedings of the 2018 Networked Privacy Workshop at CSCW, Jersey City, NJ, USA, 3–7 November 2018.
21. Millar, A.; Simeone, R.S.; Carnevale, J.T. Logic models: A systems tool for performance management. *Eval. Program Plan.* **2001**, *24*, 73–81. [CrossRef]
22. Lipkus, I.; Hollands, J. The visual communication of risk. *JNCI J. Natl. Cancer Inst.* **1999**, *91*, 149–163. [CrossRef]
23. Yin, R.K. *Case Study Research : Design and Methods*; SAGE: Los Angeles, CA, USA, 2013.
24. Mezirow, J. Transformative Learning: Theory to Practice. *New Dir. Adult Contin. Educ.* **1997**, *1997*, 5–12. [CrossRef]
25. Moon, J. Using Reflective Learning to Improve the Impact of Short Courses and Workshops. *J. Contin. Educ. Health Prof.* **2004**, *24*, 4–11. [CrossRef] [PubMed]
26. NIST. *Guide for Conducting Risk Assessments*; Technical Report SP 800-30; National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Gaithersburg, MD, USA, 2012.
27. FERMA. *A Risk Management Standard*; Technical Report; Federation of European Risk Management Associations (FERMA): Brussels, Belgium, 2003.
28. BS ISO 31000:2009. *British Standards Document BS ISO 31000:2009: Risk Management. Principles and Guidelines*; Technical Report; British Standard and the International Organization for Standardization (ISO): London, UK, 2009.
29. Virlics, A. Investment Decision Making and Risk. *Procedia Econ. Financ.* **2013**, *6*, 169–177. [CrossRef]
30. Bissonette, M. *Project Risk Management: A Practical Implementation Approach*; Project Management Institute: Newtown Square, PA, USA, 2016.
31. Lyon, B.K.; Popov, G. The Art of Assessing Risk. (cover story). *Prof. Saf.* **2016**, *61*, 40–51.
32. NIST. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*; Technical Report 800-122; National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Washington, DC, USA, 2010.

33. ISO/IEC 29100. *BS ISO/IEC29100: Information Technology—Security Techniques—Privacy Framework*; Technical Report; British Standard and the International Organization for Standardization (ISO), The International Electrotechnical Commission (IEC): London, UK, 2011.
34. Beckers, K. Comparing Privacy Requirements Engineering Approaches. In Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security (ARES), Prague, Czech Republic, 20–24 April 2012; pp. 574–581.
35. Kalloniatis, C.; Kavakli, E.; Gritzalis, S. Addressing privacy requirements in system design: The PriS method. *Requir. Eng.* **2008**, *13*, 241–255. [CrossRef]
36. Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2011**, *16*, 3–32. [CrossRef]
37. David, W.; Rachel, F.; Rowena, R. A Comparative Analysis of Privacy Impact Assessment in Six Countries. *J. Contemp. Eur. Res.* **2013**, *9*, 160–180.
38. Oetzel, M.C.; Spiekermann, S. A systematic methodology for privacy impact assessments: A design science approach. *Eur. J. Inf. Syst.* **2014**, *23*, 126. [CrossRef]
39. Information Commissioners Office. *Conducting Privacy Impact Assessments: Code of Practice*; Technical Report; Information Commissioners Office: Wilmslow, UK, 2014.
40. Westin, A.F. Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I—The Current Impact of Surveillance on Privacy. *Columbia Law Rev.* **1966**, *66*, 1003–1050. [CrossRef]
41. Solove, D.J. A taxonomy of Privacy. *Univ. Pa. Law Rev.* **2006**, *154*, 477–564. [CrossRef]
42. Palen, L.; Dourish, P. Unpacking "Privacy" for a Networked World. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI'03, Fort Lauderdale, FL, USA, 5–10 April 2003; ACM: New York, NY, USA, 2003; pp. 129–136. [CrossRef]
43. Bamberger, K.A.; Mulligan, D.K. *Privacy on the Ground: Driving Corporate Behaviour in the United States and Europe*; MIT Press: London, UK, 2015.
44. Barth, A.; Anupam, D.; Mitchell, J.C.; Nissenbaum, H.F. Privacy and contextual integrity: Framework and applications. In Proceedings of the 2006 Symposium on Security and Privacy, Berkeley/Oakland, CA, USA, 21–24 May 2006; Volume 2006, pp. 184–198. [CrossRef]
45. Amanda, C.; Anupam, D.; Nissenbaum, H.; Divya, S. Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry. *Md. Law Rev.* **2012**, *71*, 772–847.
46. Huang, H.Y.; Bashir, M. Direct-to-consumer Genetic Testing: Contextual Privacy Predicament. In Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community, American Society for Information Science, Silver Springs, MD, USA, 2015; pp. 50:1–50:10.
47. Sar, R.K.; Al-Saggaf, Y. Contextual integrity's decision heuristic and the tracking by social network sites. *Ethics Inf. Technol.* **2013**, *16*, 15–26. [CrossRef]
48. Grodzinsky, F.S.; Tavani, H.T. Privacy in "the Cloud": Applying Nissenbaum's Theory of Contextual Integrity. *SIGCAS Comput. Soc.* **2011**, *41*, 38–47. [CrossRef]
49. Krupa, Y.; Vercouter, L. Handling privacy as contextual integrity in decentralized virtual communities: The PrivaCIAS framework. *Web Intell. Agent Syst.* **2012**, *10*, 105–116. [CrossRef]
50. Hutton, L.; Henderson, T.; Kapadia, A. Short Paper: "Here I Am, Now Pay Me!": Privacy Concerns in Incentivised Location-sharing Systems. In Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless Mobile Networks, WiSec'14, Oxford, UK , 23–25 July 2014; pp. 81–86. [CrossRef]
51. Wijesekera, P.; Reardon, J.; Reyes, I.; Tsai, L.; Chen, J.W.; Good, N.; Wagner, D.; Beznosov, K.; Egelman, S. Contextualizing Privacy Decisions for Better Prediction (and Protection). In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI'18, Montreal, QC, Canada, 21–26 April 2018; ACM: New York, NY, USA, 2018; pp. 268:1–268:13. [CrossRef]