publications

MDPI

Article

A Trust Framework for Online Research Data Services

Malcolm Wolski *, Louise Howard and Joanna Richardson

Information Services, Griffith University, Nathan 4111, Australia; l.howard@griffith.edu.au (L.H.); j.richardson@griffith.edu.au (J.R.)

* Correspondence: m.wolski@griffith.edu.au; Tel.: +617-3735-4323

Academic Editor: Isabel Bernal

Received: 27 March 2017; Accepted: 30 May 2017; Published: 1 June 2017

Abstract: There is worldwide interest in the potential of open science to increase the quality, impact, and benefits of science and research. More recently, attention has been focused on aspects such as transparency, quality, and provenance, particularly in regard to data. For industry, citizens, and other researchers to participate in the open science agenda, further work needs to be undertaken to establish trust in research environments. Based on a critical review of the literature, this paper examines the issue of trust in an open science environment, using virtual laboratories as the focus for discussion. A trust framework, which has been developed from an end-user perspective, is proposed as a model for addressing relevant issues within online research data services and tools.

Keywords: virtual laboratories; science gateways; data provenance; risk perception

1. Introduction

Given the global focus on making science more transparent, reproducible, and accessible during the research process, Open Science has evolved as an umbrella term which covers various movements designed to remove "barriers to outputs, resources, methods, and tools throughout the research lifecycle. As such, open access to publications, open research data, open source software, open collaboration, open peer review, open notebooks, open educational resources, open monographs, citizen science, or research crowdfunding, fall into the boundaries of Open Science" [1].

Open Science has a high profile internationally principally because it is viewed as having "the potential to increase the quality, impact and benefits of science ... by making it more reliable, more efficient and accurate, better understandable by society and responsive to societal challenges" [2] (p. 3). The Organisation for Economic Co-operation and Development (OECD) [3] (pp. 18–19) has outlined the following rationale for/benefits of open science and open data, specifically for research and innovation: improving efficiency in science, increasing transparency and quality in the research validation process, speeding the transfer of knowledge, increasing knowledge spillovers to the economy, addressing global challenges more effectively, and promoting citizens' engagement in science and research.

In looking specifically at data, the OECD [3] (p. 18) mentions the importance of increasing both transparency and quality in the research validation process, so as to allow "a greater extent of replication and validation of scientific results". Understanding the provenance of data along with establishing rigour in regard to its management all contribute to the ultimate goal of reproducibility. The OECD goes on to discuss the quality of data in terms of a framework [4] (p. 8), of which credibility is a key dimension: "The credibility of data products refers to the confidence that users place in those products based simply on their image of the data producer, i.e., the brand image. Confidence by users is built over time. One important aspect is trust in the objectivity of the data". Nellie Kroes [5], then a vice-president of the European Commission as well as its digital agenda commissioner, has reinforced the idea that the world is moving toward a data-driven world in which trust is key. Forrester [6] (p. 10)

asserts: "In 2017, the basic fabric of trust is at stake as CEOs grapple with how to defend against escalating, dynamic security and privacy risk".

Building trust in online systems, however, is not new. According to Beldad et al. [7] (p. 857), in recent years, "both the academe and the business sector have shown a heightened interest in trust within the context of the digital environment. Knowing the nature of online trust and its determinants has become an important goal. This is obvious since online trust is regarded as a crucial factor for the success of an online enterprise or initiative". It is crucial because trust is generally assumed to be "an important precondition" for people's adoption of electronic services [7] (p. 857).

The rationale for this paper has come from the authors' desire to apply an overarching approach to the issue of trust and provenance in data services and was informed by the authors' involvement in:

- development of data services within their institution that have a public interface. For example, these include compound libraries, biobanks, health data services (e.g., clinical trials data), and general institutional research data repositories
- management of a national virtual laboratory for biodiversity and climate change modelling, where a large percentage of current users come from non-research sectors, e.g., government departments, Non-Governmental Organizations (NGOs), industry, and international users
- participation in national and international activities around the issue of trust and provenance. For example, working groups in the Research Data Alliance as well as associated national agencies, such as the Australian Data Service
- identification of imperatives and opportunities to pursue ICT service model changes, and
- earlier investigation of the impact of tools on the research data lifecycle [8]

In this paper, the authors will examine the issue of trust in an open science environment, using virtual laboratories (also known as Virtual Research Environments or Science Gateways) as a focus point. Given the apparent lack of a universally accepted definition of trust as a concept, the authors have used the following: "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [9] (p. 395). In the environment of virtual laboratories and data repositories, typically end-users will not know the people behind a system, so they will make inferences and assumptions about the people behind the system through their interactions with that system. This paper proposes a framework to (a) allow the service owner to determine what is needed to build trust and (b) provide researchers with a method of assessing what they need to look for in an online service.

2. Methodology

The authors undertook a critical review of the literature on trust as applied to several categories of online systems to determine a suitable conceptual framework for application in a research data services setting. According to Webster and Watson [10] (p. xiv), a literature review is appropriate under a number of circumstances, including the investigation of "an emerging issue that would benefit from exposure to potential theoretical foundations ... The author's contribution would arise from the fresh theoretical foundations proposed in developing a conceptual model". In their typology of reviews, Grant and Booth [11] (p. 94) have defined a critical review in terms of several key attributes: typically narrative and typically resulting in a hypothesis or model. The purpose of this type of review is to compare and evaluate a number of perspectives.

The review process was based on the following five phases. In phase one, the authors evaluated the contents of a bibliography compiled as a result of having written a recent journal article [8] on the implications for institutions, particularly universities, in supporting the increasingly complex tools which are used in the data lifecycle. Existing publications were reviewed for any specific mention of trust in relation to data services and tools.

In phase two, the authors expanded their search for additional literature, based on three broad categories. Firstly, knowledge gained from previous research had highlighted similarities between

supply chains for physical products and data products. With the increasing need to share data internationally and for systems to have a higher level of interoperability, the initial literature search used Google Scholar and was based on terms such as "supply chain", "supply chain trust", "supply chain frameworks", and "supply chain trust framework". Secondly, one of the authors' involvement with a research project on health information applied to online communities broadened the search in Google Scholar to include the terms "health information trust" and "online health information". Thirdly, the authors examined trust in e-commerce, online marketing, and e-government with particular emphasis on the end-user's perspective. Search terms included "trusted online services", "trusted data services", and "trust online data services".

In phase three, snowball sampling was used to further expand the retrieval of applicable research content through discussions with colleagues not only within Griffith University but also involved in national projects to develop virtual research environments. Designed to identify "information-rich key informants" [12] (p. 176), this technique helped to identify several key papers, including not only articles but also grey literature, which were ultimately fundamental to the design of the authors' proposed trust framework. In phase four, feedback as part of the peer review process identified data repositories as an additional category for review.

The literature examined was limited to the English language; searches were conducted between January and May 2017. The authors did not exclude any relevant publications based on format. Initially the search criterion of publication date was limited to content published since 2010, as the authors concluded that research since that date would produce the latest body of research, given the rapid growth of online services in the selected categories. Using the above terms, additional searches were conducted in the Library's Summon discovery service. All content meeting the search criteria was downloaded to a shared university network drive and allocated to a folder according to the categories identified above.

In the fifth phase, the folders were apportioned among the authors, which ensured that the full-text of the 87 downloaded publications was reviewed in an equitable manner. Regularly scheduled meetings were used to reach a consensus on which publications would be included within this critical review.

To explain the framework in a practical context, the authors have used Australian Virtual Laboratories (VLs) (https://nectar.org.au/labs-and-tools/) as a useful class of data services to provide examples of how the framework would be applied in a practical setting. These virtual laboratories (similar to Science Gateways and Virtual Research Environments in other countries) have been developed, using federal funding, to provide services to a range of research communities. They have been chosen to explain the framework as VLs typically have three components: data, software applications/infrastructure, and methods specific to their research community. They are typically open to any Australian researcher; however, the operators of the VLs may not personally know either who is using their service or the broader community who could potentially use their service. Increasingly, the VLs are being used by non-research communities, e.g., industry, government agencies, and citizen scientists.

3. Literature Review

In examining the literature about trust in online systems, the authors have focused on five main areas: industry, e-government, e-health, research data, and research data repositories.

3.1. Trust in the Industry Sector

A review of the literature specifically for industry has highlighted that trust is influenced by data. It appears there are two major categories of interest: supply chains and online retailing. In the first instance, researchers have focused on supply chain management (SCM), since there is an argument that "the market focus of competition has evolved from that of competition between individual firms

to competition between entire supply chains" [13] (p. 72). The reliance on data—and therefore data analysis—is seen to be a key to enhancing performance.

Sayogo et al. [14], in looking at a coffee supply chain, have highlighted two particular areas for further research: information security and trust. Improved trust management, for example, would address such challenges as: trust by consumers in external certifications of quality; extracting and combining trusted data from different sources; maintaining appropriate levels of stewardship of data; and creating mechanisms to ensure data integrity and security. According to Sayogo and Sahay [14,15], these may have an impact on the level of trust in the relationship between a customer and a supplier. According to Groth [16], knowing the provenance, i.e., the origin, of data in a supply chain helps consumers trust the quality of a product. Handfield's [17] (p. 8) recent research into supply chain systems concludes that "The system itself must produce data that is trustworthy".

In the second instance, trust has been identified as a key factor in the adoption of services or the sale of products from online suppliers. For example, in evaluating the importance of ratings information as part of a marketing strategy, Flanagin et al. [18] (p. 5) found that consumers were "somewhat ambivalent about whether to trust ratings and reviews". In a study of online banking, Oly Ndubisi and Kok Wah [19] (p. 542) state, "The results show that five key dimensions, namely: competence, communication, conflict handling, trust, and relationship quality, discriminate between customers in terms of perceived relationship quality and customer satisfaction."

There would seem to be a third category not well covered in the literature: companies selling data products online (e.g., services selling real estate reports on houses for sale). In these instances, issues such as data provenance and the perceived credibility of the organization are important aspects of establishing trust in the service.

3.2. Trust in the E-Government and E-Health Sectors

Trust, says Beldad et al. [7] (p. 857), is also an important factor in the adoption of e-government and e-health services. Arnold [20] (p. 140) mentions the "trust problem" in regard to integrating crowdsourced and authoritative government data. The UK government [21], in its proposed implementation of distributed ledger technology, has based its model on two key requirements: trust and interoperability. Macpherson [22] (p. 3), in his report on the analytical models that inform UK government policy, has made recommendations based on the fact that "The objective has been to ensure all models are of sufficiently high quality, and that their end users—Ministers and, ultimately, the public—can place their trust in them". Researchers, of course, contribute outputs that are used in government decision-making, e.g., policy development.

Landry et al. [23] have examined the use of open data internationally to help build urban resilience, i.e., the ability for all entities within a city to adapt to chronic and acute stressors. Key aspects are centred around trust: trusting people to make their own choices, trusted networks, trusted data sharing, and trust and reciprocity between communities.

In its report on the use of data in Australia [24] (p. 2), the Productivity Commission has concluded that "Lack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia's data. In fact, improving trust community-wide is a key objective". The Commission [24] (p. 5) highlights the health sector as exemplifying many of the opportunities widely available to use data more widely, but "to date largely foregone, due to impediments and distrust around data use" (p. 5).

Sillence et al. [25] have reported on issues associated with trust in online health information. In examining success factors for moving health promotion communities online, Sunderland et al. [26] have noted that security and trust are particularly important to health communities, and that in designing online communities to match community needs, these two concepts need to be incorporated from the beginning. Khosrowjerdi [27] (p. 189) has reinforced that "access to and trust in accountable online information is vital in the health domain".

3.3. Trust in Research Data

In establishing the basic principles which form the "Vienna Principles" for scholarly communication [28], the authors have said, in regard to quality assurance, that transparent and competent reviewing "safeguards research discoveries, ensuring that results can be trusted and built upon". However, Yoon [29] highlights that unlike scholarly outputs, such as journals and publications which have established peer review systems to validate scholarly outcomes, a similar process for data has not yet been established as a norm in data-sharing and reuse.

This is reinforced by Koeser's [30] (p. 376) assertion that "researchers effectively trust the work of others anytime they use software tools or custom software", despite the fact that "software is inherently flawed and limited". Symons and Horner [31] note that our confidence or trust in the output of a system is likely to be higher when we believe the system itself to be reliable. Reliability in software is the "probability that software will work properly in a specified environment and for a given time [32].

Proprietary software, while somewhat opaque to researchers, traditionally follows a centralised model, with updates to software code occurring only by core developers and reputation and reliability established by association with a commercial organisation. With the adoption of open (OSS) source software it was necessary to establish a new version control system [33]. In the OSS distributed model of version control, each contributor can act as a developer and may merge the work of other developers into their existing repository and publish and share updated versions. Many open source software projects and platforms have an accreditation process to verify the qualifications of candidate developers before contributions are accepted [34]. With researchers now heavily dependent on software to analyse and, at times produce, research data, establishing reliability and trust of software systems is critical. Bryant et al. [35] stated that insights obtained from computational methods would not be available without the use of software based data analytics. Software based computational models are also facilitating new research into topics where ethical or practical barriers would otherwise create restrictions [31].

One of the key elements in supporting big data, according to Demchenko et al. [36] (p. 50), is veracity. They have defined key aspects which need to be addressed to ensure data veracity, with trust figuring quite prominently:

- integrity of data and linked data (e.g., for complex hierarchical data, distributed data)
- data authenticity and (trusted) origin
- identification of both data and source
- computer and storage platform trustworthiness
- availability and timeliness
- accountability and reputation

This echoes the work of Wallis et al. [37] (p. 380), which has examined the criteria for "users to trust and interpret the data in scientific digital libraries". In a recent publication, Borgman et al. [38] have described the outcomes from a project which explored the ability of the so-called "long tail" of researchers, as exemplified by small and medium sized laboratories (SMLs), to manage their data. The results highlight the challenges of this target population in addressing the types of criteria mentioned by Demchenko and Wallis.

According to Galletta [39], given that "20 per cent of academic papers on gene research that are based on data collated in Excel spreadsheets have errors", there is a need for a monitoring and control framework, which could be applied to spreadsheets and other large files. End users need to be able to trust the accuracy, reliability, integrity, availability, and authenticity of data.

3.4. Trust in Research Data Repositories

In their article on the use of certification to establish the trustworthiness of digital repositories, Yakel et al. [40] (p. 154) make the important point that: "Trust in the repository is a separate and distinct

factor from trust in the data". Using the International Organization for Standardization (ISO) standard for Trustworthy Repositories Audit and Certification (TRAC) along with a review of the literature on both management and information systems, the authors conclude that there are two components which comprise trust and are necessary for a repository to be deemed trustworthy: trustworthy actions by repositories and trust by the stakeholders (p. 144). As a corollary, a potentially complex but important action is to understand how stakeholders construct/define trust, because this will ultimately underpin efforts to influence their trust in repositories.

For her part, Yoon [41] (p. 17) indicates that, in her survey, data repository users based their definition of trust largely on a "lack of deception". Specifically, they were influenced by data validity (or accuracy) and their perception of the "integrity" of the repository. That is, their level of understanding of the breadth of roles of repositories influenced their degree of trust in specific repositories. Similarly to Yakel et al., Yoon suggests that trust in data may not be related to trust in repositories.

Fear and Donaldson [42] have examined how proteomic researchers, interacting with data from ProteomeCommons.org, determine credibility, i.e., trustworthiness and expertise, in the context of a large, online data repository. The authors found that not only provenance metadata but also disciplinary norms play an important role in influencing the assessment of credibility. As with the other two studies, Fear and Donaldson have highlighted the importance of understanding the users'/stakeholders' perspective.

Data sharing, suggested by Nosek et al. [43], is a strong incentive for authors to make their data available openly via trusted repositories. Examples include Dataverse, Dryad, the Interuniversity Consortium for Political and Social Research (ICPSR), and the Open Science Framework (OSF). At the same time, a major impediment to data publishing is the cost incurred in actually establishing a trustworthy repository which both archives and makes accessible the data [44].

At the international level, there are a number of special interest groups within the Research Data Alliance (https://www.rd-alliance.org/) which focus on repositories. In particular, the purpose of the Preservation e-Infrastructure IG is "to reach wide agreement on the e-Infrastructure services which are needed to help repositories to preserve their data holdings, to ensure the interoperability of service implementations, and to build trust of service providers". The International Organization for Standardization (RDA/WDS) Certification of Digital Repositories IG promotes certification as it is "fundamental in guaranteeing the trustworthiness of digital repositories and thus in sustaining the opportunities for long-term data sharing".

3.5. Trust Frameworks

Rousseau et al. [9] introduced a three dimensional framework for the analysis of trust. In the first dimension lies the propensity of individuals to trust. The second covers the facets of trustworthy behaviour and is grounded in an evaluation of people's ability, integrity, and benevolence. The third dimension is defined by levels of trust development achieved and builds along a continuum of hierarchical and sequential stages such that, as trust grows to higher levels, it becomes stronger and more resilient and changes in character.

Selnes [45] (p. 311) introduced a four-part model, in which "Competence and communication are proposed to drive trust, whereas communication, commitment, and conflict handling drives satisfaction". This model was subsequently expanded by Morris and Hunt [46] to include a fifth component: culture.

Having compared various definitions of trust across research disciplines, Handfield [47] (p. 1) asserted that trust could be grouped into six "conceptual paradigms": reliability, competence, goodwill (openness and benevolence), vulnerability, loyalty, and multiple forms of trust (as defined by cognitive trust and affective faith trust). Gefen and Straub [48] (p. 408) discussed trust as "an *interpersonal* determinant of behavior that deals with beliefs about ... integrity, benevolence, ability, and predictability." In an online context, they focus on four attributes of what they call "e-Trust": integrity, benevolence, ability, and predictability.

Tan et al. [49] (p. 2) identified three trustworthiness factors as "trust-inducing antecedents" specifically in relation to websites; however, the following are equally applicable more generally to online systems and services:

- Ability: Degree to which an individual customer believes that the website has the ability, skills, and expertise to perform effectively in specific domains
- Benevolence: Degree to which an individual customer believes that the website cares about him/her and acts in his/her interests, and
- Integrity: Degree to which an individual customer believes that the website adheres to a set of principles that he/she finds acceptable

In a conference presentation in 2015 on spatial data, Arnold [50] reinforced the desirability for what he referred to as "trust models", particularly in regard to accepting crowdsourced data. For his part, Khosrowjerdi [27] has reported on 12 theory-driven models of trust specifically in the online health context, the results of which have highlighted the complexity of health information-seeking behaviour.

Although not strictly a "trust framework", the work undertaken by McIntosh et al. [51] in the area of reproducibility of biomedical research offers a good example of emerging discipline-specific "checklists"/standard processes, which could fit under a trust model. The Repeatability Assessment Tool (RepeAT) Framework is made up of a range of variables classified according to five major categories: research design and aim; database and data collection methods; data mining and data cleaning; data analysis; and data sharing and documentation. The ultimate goal is to identify practices which, when adopted by researchers, address concerns (lack of trust) regarding the reliability and verifiability of biomedical research outputs.

The review of the literature has identified a number of trust models applied to the non-research sector; however, no trust model or framework was found that had been applied specifically to online research data services/tools. This paper addresses that gap.

4. Proposed Trust Framework for Online Research Services

From the review of the literature, the authors felt that the model proposed by Morris and Hunt [46] was the one most suited for the online research data environments, particularly because it had been applied specifically to a research environment, i.e., university-industry research collaboration. Based on the four determinants introduced by Selnes [45], Morris and Hunt added a fifth determinant: culture. Culture is seen as an additional critical element not only in an open science environment but also to accommodate an increasingly diverse range of stakeholders. Therefore, the framework proposed below is comprised of those five determinants to establish trust, as the basis on which research service owners need to focus. These determinants are: competence, conflict handling, communications, culture, and commitment.

The above framework addresses the trust issue from the point of view of the end-user. This is deliberate. In the online environment, it is the end-user who must be satisfied that their expectations are being met before they will trust the service. What they see on the online service website, plus the subsequent experience, will determine their level of trust in the service. This paper focuses on the research environment, in which the end-user is predominantly a researcher, while recognising that increasingly that end-user could be an industry user, student, librarian, or other support staff member attempting to determine whether the service would/should be used.

These determinants are discussed in detail in the following sections. The proposed framework is applicable for all online research tools/services. In particular, this paper is most interested in the applicability for tools/services that deliver data products of some nature.

As discussed earlier, the authors have used Australian Virtual Laboratories (VLs) to help explain the model and its application by providing examples, where appropriate, in the following sections.

Similar to many commercial services, e.g., Amazon, one objective of the VLs should be to build an ongoing relationship with users. This is relevant in research, for reasons such as:

(a) The service owners rely directly or indirectly on the end-users to help attract further funding (e.g., grants);
(b) The numbers of users are an indication of uptake to demonstrate a return on investment; and
(c) The end-user community is the source of knowledge with which to further develop the product. Many research services are on the upward side of the maturity curve [52] and need further development and innovation.

One core objective of a trust framework is to build trusted relationships. To establish trust through these five determinants, the literature has also highlighted a number of aspects that service owners need to take into account when applying the framework to their own circumstances. Using the virtual laboratories as a class of data services, system owners will respond to meet the expectations in the five determinants through strategies to improve provenance, quality, governance, rigor, and maturity of the service. These strategic responses are common to most organisations selling services and products online or, for that matter, internal groups providing internal enterprise systems services.

In the sections below, each determinant of the framework is explained. A range of applicable strategies have been identified in parentheses.

4.1. Competence

In essence, building trust through perceptions about competence is addressed by providing evidence to give the end-user confidence that the service provider can do what they promise, in the absence of any previous personal direct experience with the service or the people behind the service. While transparency and openness are key attributes of Open Science, they have to be complemented by a "QA" or review process to demonstrate competence. In the context of a VL, this could be achieved in several ways:

- information available about governance, such as objectives, development plan, partnerships, governance structure (governance, maturity, rigor);
- documented evidence on sources of methods, data, and tools (quality, rigor);
- documented levels of service provided to end-users (quality, maturity, rigor);
- evidence of quality in processes in their development and support, and processes to ensure data quality (quality, maturity, rigor);
- citeability of data, tools, and methods used for reproducibility purposes (quality, rigor);
- evidence of peer review processes for methods and data quality (quality, rigor);
- if it is a federated system, evidence on how the inter-organisational processes and governance operates (quality, provenance, governance);
- evidence of best practices, e.g., ISO standards, conventions, etc. (quality, maturity, rigor); and
- evidence of security, privacy, and other legal compliances (maturity, rigor).

4.2. Culture

Culture has specific relevance in the research environment. The culture of the organisation providing the service has to align with the expectations of the various stakeholders, including end-users. If the end-user perceives that the culture of the service provider and its underpinning partners do not align with their own expectations, this may make it more difficult to build trust. An organisation with a strong for-profit culture may find it difficult to build trust among end-users in a not-for-profit community. Similarly, a service provider regarded as unapproachable might find it difficult to build trust. Phan et al. [53] write about benevolent trust, where each partner must exhibit a behavioural tendency toward helping and supporting the other partner, a tendency to promote and seek closeness with the other partner by encouraging sharing, understanding, mutual interest, and openness. Research institutions and universities have a benevolent level of trust inbuilt because of their inherent mission.

In the current environment, openness and transparency are a critical part of the process in building trust and will need to be demonstrated by the service provider.

An example of the impact of perceptions about culture would be to compare end-users' expectations about the collaborative nature of a medical research institution versus a commercial for-profit organisation, such as a health insurance company. In the context of the VL environment servicing a specific community, this may be achieved through emphasising characteristics such as:

- publishing how feedback is collected and incorporated into future development (governance, quality);
- published mission/vision and/or objectives (maturity, quality);
- holding workshops and webinars targeting specific end-user application problems (maturity);
- publishing user-stories (maturity, rigor);
- demonstrating the professionalism of the team and their roles, e.g., scientific, IT, and other key stakeholders (quality, maturity, rigor);
- demonstrating open science characteristics and transparency of operations (governance, rigor, maturity); and
- highlighting any partnerships with existing, recognisable, trusted organisations (maturity, rigor, quality).

4.3. Commitment

Commitment has been identified as a key characteristic in building trusting relationships. In its basic sense, the two parties expect each other to be committed to what they have in common [45]. From an end-user's perception, their satisfaction levels are determined by how well the service meets their needs. In the absence of any personal connection, the online service provider will need to show that commitment through the website. This can be shown through evidence such as:

- the robustness of the products offered, such as uptime/downtime, bug fixes, quality of the product (maturity, quality, rigor);
- documented terms of service (maturity, governance);
- documented agreements between partners who provide the service and its various components, such as data providers, researchers' institutions providing the discipline know-how, and the application developer/maintenance (maturity, governance);
- the maturity or quality of the institutions involved (e.g., is the service managed through project funds or managed by an organisation that has longevity) (maturity, governance); and
- the lived experience of the user.

4.4. Conflict Resolution

Conflict resolution is crucial for maintaining a good trusting relationship. It could arise from different perceptions and expectations about goals or levels of services through to system failures or simple system faults. These can be destructive, if not handled correctly. Conversely, Selnes [45] (p. 310) notes that "total suppression of conflict can result in a relationship that loses vitality and does not develop into a more fruitful cooperation". Gundlach and Murphy [54] also highlighted that purchasers of products have an expectation that the service owner has obligations for any unforeseen and unplanned events that may not have been specifically covered in any contracts or agreements for services. This goes beyond resolving known conflicts. It is the service provider's ability to minimize the negative impacts of not only actual conflicts but also potential conflicts before they become problems. In the commercial world, the vendor may just provide a refund or replace the product. The way a service provider handles conflict can directly impact satisfaction and consequently the level of trust in the service. In the context of the research environment and VLs, this becomes a more interesting problem to solve. Suggested examples of how to build trust through this element would be:

- help desk services in place with documented response and escalation levels (maturity, governance);
- use of peer support in cases of user error (maturity);
- outage and known problem listed (governance, maturity);
- evidence of community testing or alpha and beta releases of new functionality to obtain feedback to pre-empt problems (maturity, rigor);
- whether the end-user license agreements/service levels specify commitment and processes in the case of conflict (maturity, governance);
- evidence of reporting conflicts and problems to the governance groups (maturity, governance); and
- transparency about how known problems are being addressed or, in some cases, not being addressed with reasons (maturity, governance).

4.5. Communication

Communication between the service provider and the end-user is critical and it needs to happen at all levels. A simple example is communication on transactions which, in the commercial world, could be a communication that your order has been placed, another once it is shipped, and another when it arrives, etc. Communication is an important source of satisfaction, which is also a determinant of trust, i.e., the more one is satisfied with the service, the more the service owner is trusted [45].

In the research environment, it is even more critical to develop transparency and openness. Because language is so imperfect and the range of potential users of some services is broad, an open dialogue is often a necessity in addition to static information on online systems. This open dialogue is essential for developing and preserving a shared understanding of the relationship and thus preserves trust [55]. Increasingly, as applications become more mobile and communication channels become more dynamic, service providers need to use these more dynamic channels to communicate with their community. User expectations about responsiveness are becoming more real-time.

Research environments offer one more twist in that they are increasingly becoming more federated. For example, an online service for researchers may provide data supplied from a partner, as well as utilise tools and methods from elsewhere through web services. In these instances, there needs to be effective and open communication between these partners.

In the context of VLs, communication may be addressed through:

- In its simplest form, good communication through a transaction cycle, e.g., email updates on the progress of experiments or requests made (quality, rigor);
- An online interface that openly and easily provides evidence, as required (governance, maturity);
- Newsletters/blogs on usage, development plans, user stories, chat windows, etc., that promote an open dialogue with end-users (maturity, quality);
- Publishing of all provenance information about data, tools, and methods and, if necessary, documentation as to how it was determined (provenance, rigor);
- If a federated system, reporting on usage and performance backwards and forwards among key partners in the system (governance, rigor and maturity);
- Is it clear which organisations are backing the service, e.g., reputation/branding (maturity, governance); and
- Communicating a continuous improvement cycle through end-user feedback (quality, commitment).

The example responses above in one determinant have overlap in another. Some of the examples are useful to build trust across several determinants, e.g., adherence to an international convention may not only establish commitment but also is useful to build trust around the culture. As a system owner responds by implementing strategies to develop trust, momentum builds as early efforts can have a compound effect over time. For example, involving the right partners early can help establish the commitment to the service, and leveraging the "brand" of those partners can help establish the service "brand".

4.6. Perception of Risk

In the research environment, not all tools or services need a high level of trust, as, in some cases, fit-for-purpose is a more practical response because of the low risk. However, perceived risk can directly impact on consumers' attitudes and intentions towards the use of technology based services [56]. Where consumers perceive risk to be high, establishing trust is essential to reducing the level of risk perceived [57]. A determination of how much effort and resources will be required to address the problem can only be developed by looking at the risk profile of the system from both the system owner's point of view and the end-user's point of view. Trust in the service is often dependent on whether the one who is trusting believes there are impersonal and institutional structures in place to ensure the success of a transaction [58]. To assess the risk, service owners can use well established risk management approaches, which are used by most mature organisations.

Online research environments, however, potentially have a diverse user community, ranging from users from government, industry, and non-government organisations to individual researchers, students, citizen scientists, and members of the public (across all age groups and nationalities). Zhu and Chang [59] identified that, unlike physical goods, consumers struggle to form an accurate assessment of technology-based services. Risk perception is also influenced by factors specific to the online environment, such as the fear of unauthorised access to systems and data security and loss [60].

While a service owner may apply established organisational risk management approaches to determine the level of effort, it is worth remembering that end-users perceive the risks in different ways and apply different value propositions. End-users' assessments of an online service's risk of usage include a perceived usefulness and perceived ease-of-use element, as well as a social influence factor [61]. Hengstler et al. [57] found that communication was more effective in reducing the level of perceived risk when translated for different target groups and when the application and purpose of technology was explained. Many authors highlight the relationship between trust, satisfaction, and perceived risk [62]. Kim and Lennon [63] have identified a link between reputation and website quality as a contributor to reducing perceived risk and eliciting positive emotion, which eventually leads to purchase intention.

Martin et al. [64] highlight the importance of establishing trust and satisfaction in online shopping to reduce perceived risks, particularly amongst infrequent users. They also recommend two e-retail strategies: (a) develop risk reduction strategies, such as improving conflict handling processes, and (b) target satisfaction building activities built into the site to positively influence affective experience states, e.g., ease-of-use, personalisation/customisation, connectedness, aesthetics, and improving perceived benefits. Fethermann and Pavlou [65] also highlighted that end-users will tolerate higher levels of risk if they perceive that they have a level of control over the environment (e.g., advising users of the level of security and privacy in-built into the system and advice on how the end-user can use the system securely). In addition, Kim and Lennon [63] noted that online retailers should incorporate online features that reduce consumers' perceived risk of shopping on the web site by enhancing customer service, providing adequate product and security information, and building a reputation of a reliable company.

These additional factors around risk reduction and satisfaction building should be considered in developing a response to the trust framework. Given the importance of the end-users' perceptions in developing trust, the communication determinant in the trust framework becomes an important focus in building relationships with end-users. Also noted is the impact of social influence on end-users' perceived risk level. For example, testimonials from peers could have a positive effect on perceived usage [66]. In light of perceptions about risk in an online environment, service owners should reflect on priorities about which cohort of end-users the planned response should target first.

5. Discussion

Building a trusted service does not happen overnight and requires time, a plan and, typically, resources for ongoing operations. For services to have a high level of trust, they must be sustainable

operations. As services such as VLs scale up to service large communities, they will need staff to provide support and administrative functions around the system, not unlike typical enterprise systems or online shopping sites. Jisc [67] has discussed this in considerable detail in its guide on implementing a virtual research environment. In addition, as the previous discussion shows, efforts can have a compound effect across the determinants; so, early efforts may pay dividends further down the track.

The above framework in Figure 1 can be used for several practical purposes by several stakeholder groups:

- Funders can use it to determine how much effort and resources are required to build the required level of trust in the relevant services;
- Researchers and other end-users can use it to determine whether they will use the service; and
- Support and outreach staff can use it as a guide to provide advice to their researcher (and other end-user) cohorts. In a university, this is somewhat similar to services already being provided by librarians in regard to resources to determine literature and journal quality.

The limitation of the framework is that it has broad application and is not prescriptive, as the application of the framework needs to be designed to address each specific service on a case-by-case basis. The governance group of a research service needs to determine the appropriate level of response. This is because the members have the specific knowledge required to apply the framework to their particular environment. In the case of the VLs, it would be expected that responses would need to be developed as part of a multi-year plan because of resource commitments and the time required to develop additional processes.

While the discussion has focused on VLs, the proposed framework is applicable to any online research tool used by researchers. For example, Kramer and Bosman [68] have extensively researched the use of tools by researchers and have identified over 600. Over 70% of these tools are single phase tools in the research data lifecycle. The percentage of new, single use tools in the last four years is close to 80% [8]. The proposed framework would also be useful in these cases.

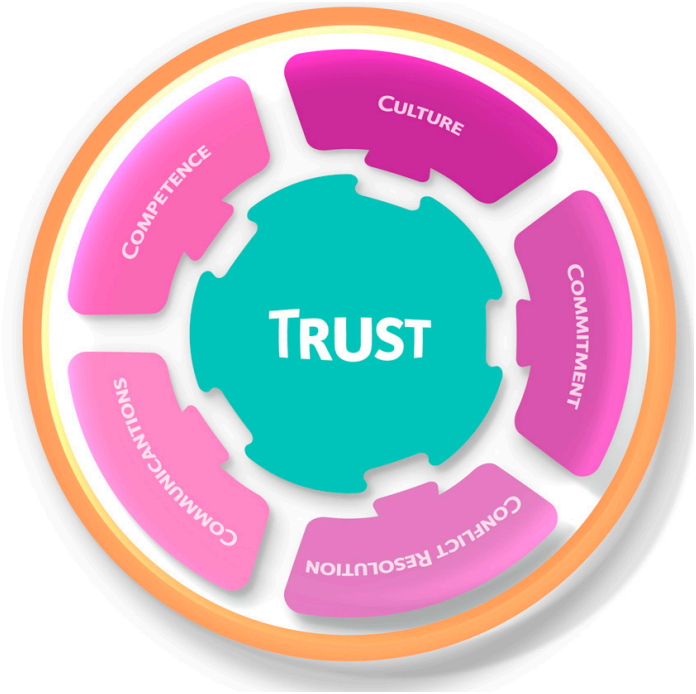

Figure 1. Trust Framework for Research Services/Tools.

This framework has been developed from an end-user's perspective and is based on the large amount of literature on the topic of the use of online services in industry and government. The next step would be to apply this framework to an existing service as a case study of its practical application, commencing with the development of a trust plan. The discussion has also highlighted the key role that the online environment plays in building trust both in content and design. An additional factor is the need for ongoing resources to support engagement as user expectations become more "real time" in nature.

Tackling the issue of building trusted services has many side-benefits, as it also addresses other topical issues, such as developing rigor into science, reproducibility, open science more broadly, and good governance.

6. Conclusions

For industry, citizens, and other researchers to participate in the open science agenda, further work needs to be undertaken to establish trust in research environments. This is especially critical to those online services delivering data products. As this paper shows, developing trust and a trusted relationship with end-users takes time and effort. This needs to be recognised by both funders and service owner governance bodies when committing resources and setting priorities.

This paper has also highlighted the need for service owners to understand the perceptions and characteristics of their end-user cohorts when developing their plan using the trust framework.

Further study is needed on understanding the relationship between trust, risk, satisfaction, perceived ease of use, and perceived user benefits between the different cohort user groups in specific research domains to assist in development strategies of online research services (e.g., population health, genomics). This is essential if research communities are planning to increase industry and citizen uptake of their data product as well as broaden the research user community across disciplines.

Author Contributions: All authors contributed equally to the literature review and the development and analysis of the proposed model.

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

References

1. Bueno de la Fuente, G. What is Open Science? Introduction. Available online: https://www.fosteropenscience.eu/content/what-open-science-introduction (accessed on 20 May 2017).
2. Council of the European Union. *Outcome of Proceedings. 27 May 2016*; The Council: Brussels, Belgium, 2016. Available online: http://data.consilium.europa.eu/doc/document/ST-9526-2016-INIT/en/pdf (accessed on 20 May 2017).
3. OECD. *Making Open Science a Reality*; OECD Science, Technology and Industry Policy Papers, 25; OECD Publishing: Paris, France, 2015.
4. OECD. *Quality Framework and Guidelines for OECD Statistical Activities*; OECD: Paris, France, 2012. Available online: http://www.oecd.org/officialdocuments/displaydocumentpdf/?cote=std/qfs(2011)1&doclanguage=en (accessed on 20 May 2017).
5. Kroes, N. A Secure Online Network for Europe. Speech Delivered at EU Cybersecurity Strategy—High Level Conference, Brussels, Belgium, 28 February 2014. Available online: http://europa.eu/rapid/press-release_SPEECH-14-167_en.htm (accessed on 20 May 2017).
6. Forrester Research. *2017 Predictions: Dynamics That Will Shape the Future in the Age of the Customer*; Forrester: Cambridge, MA, USA, 2016.
7. Beldad, A.; De Jong, M.; Steehouder, M. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Comput. Hum. Behav.* **2010**, *26*, 857–869. [CrossRef]
8. Wolski, M.; Howard, L.; Richardson, J. The Importance of Tools in the Research Data Lifecycle. *Digit. Libr. Perspect.* **2017**, *33*, in press.
9. Rousseau, D.M.; Sitkin, S.B.; Burt, R.S.; Camerer, C. Not so different after all: A cross-discipline view of trust. *Acad. Manag. Rev.* **1998**, *23*, 393–404. [CrossRef]

10. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, xiii–xxiii.
11. Grant, M.J.; Booth, A. A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Inf. Libr. J.* **2009**, *26*, 91–108. [CrossRef] [PubMed]
12. Patton, M.Q. *Qualitative Evaluation and Research Methods*; Sage: Newbury Park, CA, USA, 1990.
13. Hazen, B.T.; Boone, C.A.; Ezell, J.D.; Jones-Farmer, L.A. Data quality for data science, predictive analytics, and big data in supply chain management: An introduction to the problem and suggestions for research and applications. *Int. J. Prod. Econ.* **2014**, *154*, 72–80. [CrossRef]
14. Sayogo, D.S.; Zhang, J.; Luna-Reyes, L.; Jarman, H.; Tayi, G.; Andersen, D.L.; Pardo, T.A.; Andersen, D.F. Challenges and requirements for developing data architecture supporting integration of sustainable supply chains. *Inf. Technol. Manag.* **2015**, *16*, 5–18. [CrossRef]
15. Sahay, B.S. Understanding trust in supply chain relationships. *Ind. Manag. Data Syst.* **2003**, *103*, 553–563. [CrossRef]
16. Groth, P. Transparency and reliability in the data supply chain. *IEEE Internet Comput.* **2013**, *17*, 69–71. [CrossRef]
17. Handfield, R. Preparing for the Era of the Digitally Transparent Supply Chain: A Call to Research in a New Kind of Journal. *Logistics* **2016**, *1*, 2. [CrossRef]
18. Flanagin, A.J.; Metzger, M.J.; Pure, R.; Markov, A.; Hartsell, E. Mitigating risk in ecommerce transactions: Perceptions of information credibility and the role of user-generated ratings in product quality and purchase intention. *Electron. Commer. Res.* **2014**, *14*, 1–23. [CrossRef]
19. Oly Ndubisi, N.; Kok Wah, C. Factorial and discriminant analyses of the underpinnings of relationship marketing and customer satisfaction. *Int. J. Bank Mark.* **2005**, *23*, 542–557. [CrossRef]
20. Arnold, L. Improving spatial data supply chains: Learnings from the manufacturing industry. In *Proceedings of GEOProcessing 2016*; Curran Associates: Red Hook, NY, USA, 2016; pp. 137–145. Available online: https://www.thinkmind.org/download.php?articleid=geoprocessing_2016_9_10_30106 (accessed on 15 May 2017).
21. Walport, M. *Distributed Ledger Technology: Beyond Blockchain*; Government Office for Science: London, UK, 2016. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (accessed on 20 May 2017).
22. Maccpherson, N. *Review of Quality Assurance of Government Analytical Models: Final Report*; HM Treasury: Westminster, UK, 2013. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206946/review_of_qa_of_govt_analytical_models_final_report_040313.pdf (accessed on 15 May 2017).
23. Landry, J.-N.; Webster, K.; Wylie, B.; Robinson, P. *How Can We Improve Urban Resilience with Open Data?* Open Data Institute: London, UK, 2016. Available online: http://www.urenio.org/2016/12/23/can-improve-urban-resilience-open-data/ (accessed on 20 May 2017).
24. Australian Government. *Productivity Commission. Data Availability and Use*; Productivity Commission: Canberra, Australia, 2017. Available online: http://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf (accessed on 20 May 2017).
25. Sillence, E.; Briggs, P.; Harris, P.; Fishwick, L. A framework for understanding trust factors in web-based health advice. *Int. J. Hum. Comput. Stud.* **2006**, *64*, 697–713. [CrossRef]
26. Sunderland, N.; Beekhuyzen, J.; Kendall, E.; Wolski, M. Moving health promotion communities online: A review of the literature. *Health Inf. Manag. J.* **2013**, *42*, 9–16. [CrossRef]
27. Khosrowjerdi, M. A review of theory-driven models of trust in the online health context. *IFLA J. Int. Fed. Libr.* **2016**, *42*, 189–206. [CrossRef]
28. Kraker, P.; Dörler, D.; Ferus, A.; Gutounig, R.; Heigl, F.; Kaier, C.; Rieck, K.; Šimukovič, E.; Vignoli, M. The Vienna Principles: A Vision for Scholarly Communication in the 21st Century. Available online: http://viennaprinciples.org/ (accessed on 20 May 2017).
29. Yoon, A. Data reusers' trust development. *J. Assoc. Inf. Sci. Technol.* **2017**, *68*, 946–956. [CrossRef]
30. Koeser, R.S. Trusting Others to 'Do the Math'. *Interdiscipl. Sci. Rev.* **2015**, *40*, 376–392. [CrossRef] [PubMed]
31. Symons, J.; Horner, J. Software intensive science. *Philos. Technol.* **2014**, *27*, 461–477. [CrossRef]
32. Voas, J.; Hurlburt, G. Third-Party Software's Trust Quagmire. *Computer* **2015**, *48*, 80–87. [CrossRef] [PubMed]
33. Orsila, H.; Geldenhuys, J.; Ruokonen, A.; Hammouda, I. Trust issues in open source software development. In *Proceedings of the Warm Up Workshop for ACM/IEEE ICSE 2010*; ACM: New York, NY, USA, 2009; pp. 9–12.

34. Ho, S.Y.; Richardson, A. Trust and distrust in open source software development. *J. Comput. Inform. Syst.* **2013**, *54*, 84–93. [CrossRef]
35. Bryant, R.; Katz, R.H.; Lazowska, E.D. Big-Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society. 2008. Available online: https://pdfs.semanticscholar.org/65a8/b00f712ffd5c230bf0de6b9bd13923d20078.pdf (accessed on 20 March 2017).
36. Demchenko, Y.; Grosso, P.; De Laat, C.; Membrey, P. Addressing big data issues in scientific data infrastructure. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 20–24 May 2013; pp. 48–55.
37. Wallis, J.C.; Borgman, C.L.; Mayernik, M.S.; Pepe, A.; Ramanathan, N.; Hansen, M. Know thy sensor: Trust, data quality, and data integrity in scientific digital libraries. In *International Conference on Theory and Practice of Digital Libraries*; Springer: Berlin, Germany, 2007; pp. 380–391.
38. Borgman, C.L.; Golshan, M.S.; Sands, A.E.; Wallis, J.C.; Cummings, R.L.; Darch, P.T.; Randles, B.M. Data management in the long tail: Science, software, and service. *Int. J. Digit. Curation* **2016**, *11*, 128–149. [CrossRef]
39. Galletta, J. Ensuring Data Accuracy in Research Organisations. *Res. Inf. J.* **2017**. Available online: https://www.researchinformation.info/news/analysis-opinion/ensuring-data-accuracy-research-organisations (accessed on 20 May 2017).
40. Yakel, E.; Faniel, I.; Kriesberg, A.; Yoon, A. Trust in digital repositories. *Int. J. Digit. Curation* **2013**, *8*, 143–156. [CrossRef]
41. Yoon, A. End users' trust in data repositories: Definition and influences on trust development. *Arch. Sci.* **2014**, *14*, 17–34. [CrossRef]
42. Fear, K.; Donaldson, D.R. Provenance and credibility in scientific data repositories. *Arch. Sci.* **2012**, *12*, 319–339. [CrossRef]
43. Nosek, B.A.; Alter, G.; Banks, G.C.; Borsboom, D.; Bowman, S.D.; Breckler, S.J.; Contestabile, M. Promoting an open research culture. *Science* **2015**, *348*, 1422–1425. Available online: http://science.sciencemag.org/content/348/6242/1422 (accessed on 20 May 2017). [CrossRef] [PubMed]
44. Assante, M.; Candela, L.; Castelli, D.; Tani, A. Are scientific data repositories coping with research data publishing? *Data Sci. J.* **2016**, *15*, 6.
45. Selnes, F. Antecedents and consequences of trust and satisfaction in buyer-seller relationships. *Eur. J. Mark.* **1998**, *32*, 305–322. [CrossRef]
46. Morris, B.; Hunt, R. Trust and Distrust in University-Industry Research Collaborations. In *Proceedings of the 22nd ANZAM Conference: Managing in the Pacific Century*; Promaco Conventions: Auckland, New Zealand, 2008; pp. 1–21. Available online: http://hdl.handle.net/1959.14/173595 (accessed on 20 March 2017).
47. Handfield, R. *Trust in Supply Chain Relationships: What Does It Mean to Trust?—Part I*; North Carolina State University Supply Chain Resource Cooperative: Raleigh, NC, USA, 2003. Available online: https://scm.ncsu.edu/scm-articles/article/trust-in-supply-chain-relationships-what-does-it-mean-to-trust-part-i (accessed on 20 May 2017).
48. Gefen, D.; Straub, D.W. Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega* **2004**, *32*, 407–424. [CrossRef]
49. Tan, C.W.; Benbasat, I.; Cenfetelli, R.T. Building citizen trust towards e-government services: Do high quality websites matter? In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 7–10 January 2008; p. 217.
50. Arnold, L. Spatial Data Supply Chains: Towards a National Spatial Data Supply Chain. Presentation at Locate15, Brisbane, Australian, 10–12 March 2015. Available online: http://www.crcsi.com.au/assets/Uploads/Towards-a-national-spatial-data-supply-chain-March-2015.pdf (accessed on 20 May 2017).
51. McIntosh, L.D.; Juehne, A.; Vitale, C.R.H.; Liu, X.; Alscoser, R.; Lukas, J.C.; Evanoff, B. Repeat: A Framework to Assess Empirical Reproducibility in Biomedical Research. 2017. Available online: https://osf.io/4np66/ (accessed on 31 May 2017).
52. Fenn, J.; Raskino, M. *Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time*; Harvard Business Press: Boston, MA, USA, 2008.
53. Phan, M.C.T.; Styles, C.W.; Patterson, P.G. Relational competency's role in Southeast Asia business partnerships. *J. Bus. Res.* **2005**, *58*, 173–184. [CrossRef]

54. Gundlach, G.T.; Murphy, P.E. Ethical and legal foundations of relational marketing exchanges. *J. Mark.* **1993**, *57*, 35–46. [CrossRef]
55. Sabel, C.F. Studied trust: Building new forms of cooperation in a volatile economy. *Hum. Relat.* **1993**, *46*, 1133–1170. [CrossRef]
56. Schaupp, L.C.; Carter, L.D. Antecedents to e-file adoption: The US citizen's perspective. *eJ. Tax Res.* **2009**, *7*, 158.
57. Hengstler, M.E.; Duelli, S. Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. *Technol. Forecast. Soc.* **2016**, *105*, 105–120. [CrossRef]
58. McKnight, D.H.; Cummings, L.L.; Chervany, N.L. Initial trust formation in new organizational relationships. *Acad. Manag. Rev.* **1998**, *23*, 473–490.
59. Zhu, D.H.; Chang, Y.P. Investigating consumer attitude and intention toward free trials of technology-based services. *Comput. Hum. Behav.* **2014**, *30*, 328–334. [CrossRef]
60. Paluch, S.; Wünderlich, N.V. Contrasting risk perceptions of technology-based service innovations in inter-organizational settings. *J. Bus. Res.* **2016**, *69*, 2424–2431. [CrossRef]
61. Featherman, M.S.; Hajli, N. Self-service technologies and e-services risks in social commerce era. *J. Bus. Ethics* **2016**, *139*, 251–269. [CrossRef]
62. Chen, C. Perceived risk, usage frequency of mobile banking services. *Manag. Serv. Qual.* **2013**, *23*, 410–436. [CrossRef]
63. Kim, J.; Lennon, S.J. Effects of reputation and website quality on online consumers' emotion, perceived risk and purchase intention: Based on the stimulus-organism-response model. *J. Res. Int. Mark.* **2013**, *7*, 33–56. [CrossRef]
64. Martin, J.; Mortimer, G.; Andrews, L. Re-examining online customer experience to include purchase frequency and perceived risk. *J. Retail. Consum. Ser.* **2015**, *25*, 81–95. [CrossRef]
65. Featherman, M.S.; Pavlou, P.A. Predicting e-services adoption: A perceived risk facets perspective. *Int. J. Hum. Comput. St.* **2003**, *59*, 451–474. [CrossRef]
66. Hickson, S.; Poulton, K.A.; Connor, M.; Richardson, J.; Wolski, M. Modifying researchers' data management practices: A behavioural framework for library practitioners. *IFLA J. Int. Fed. Libr.* **2016**, *42*, 253–265. [CrossRef]
67. Brown, C. *Implementing a Virtual Research Environment (VRE)*; Jisc: Bristol, UK, 2013. Available online: https://www.jisc.ac.uk/full-guide/implementing-a-virtual-research-environment-vre (accessed on 20 May 2017).
68. Kramer, B.; Bosman, J. Innovations in scholarly communication-global survey on research tool usage. *F1000Research* **2016**, *5*. [CrossRef] [PubMed]