Raising Trust in the Food Supply Chain

Alexander Krumpholz, Marthie Grobler, Raj Gaire, Claire Mason and Shanae Burns
CSIRO Data61, Australia
[firstname.lastname]@data61.csiro.au

***Abstract*—With more devices connected to the internet, collecting and sharing data using the Internet of Things (IoT) is an exciting prospect for many food supply chain stakeholders and consumers. However, new technologies introduce significant real and perceived security and privacy concerns that are hindering broader adoption of these technologies. While many of these risks can be mitigated through advanced privacy preservation technologies and security practices, we hypothesized that participants in primary industry supply chains have limited knowledge of these tools. By investigating perceptions and attitudes towards data sharing and privacy preserving tools, we hoped to reveal how communication strategies could be targeted to address this barrier to usable security in data sharing and digital food supply chains. To this end, we carried out pilot interviews and conducted a survey of Australian food supply chain stakeholders to explore: (1) current data sharing practices and the attitudes of food supply chains participants towards such practices, and (2) the perception towards privacy preserving techniques. We found that the extent of data sharing differs among different food supply chains. In general, participants in these supply chains were cautiously positive about the potential for data sharing. They also report that they were developing more trust in privacy preserving technologies as a tool for managing data sharing risk. An issue that emerged was the perception that the effort required to engage with data sharing platforms outweighs the benefits derived from them. Furthermore, the benefits of data sharing were not seen to be evenly distributed across the supply chain. These findings provide useful direction for progressing the adoption of digital supply chains.**

I. Introduction

The data revolution powered by the Internet of Things (IoT) is considered as the key to effective decision making, particularly in supply chains, with the gains from timely and accurate data providing insights into the current state and reliable predictions for future directions. Consumers now put new demands on attributes such as price, quality, integrity and safety [18] that need sharing data among supply chain participants. However, the cost of data collection, management and communication, benefit distribution and loss of competitive advantage due to information asymmetry can create barriers to data sharing. Besides, the management and handling of data, particularly data related to private and confidential aspects of commerce, is not universally regulated within the supply chain environment. The acceptance of technology to share information also largely depends on the knowledge and perceptions of supply chain participants regarding their data sharing practices and privacy preserving technologies. Therefore, a study on these factors is vital to ensure that usable security is incorporated into digital agriculture systems.

This exploratory study takes a deeper look into current data sharing practices in the traditionally non-digital food supply chain in Australia. We investigate the role that privacy/confidentiality and privacy preserving techniques play in adopting data sharing practices, particularly among farmers and producers. This study contributes the identification of existing social and technical barriers as perceived by supply chain participants in terms of data sharing and privacy, as well as a better understanding of the pain points relevant to the supply chain's online data sharing incentives. We find that the supply chain of food products tends to take on a very one-directional downstream approach, with both products and data mostly only being shared from farmers to the end users and consumers, and rarely, if at all, shared upstream, from the end users and consumers to the original suppliers. In addition to the obvious communication barriers introduced with such a one-directional information flow, usable security in the context of online privacy and security is often a much-neglected aspect in these supply chains. We argue that data sharing within a supply chain necessitates a dynamic view of privacy, adapting based on the risk profile of the individual supply chain entity whilst justifying the need and the benefit to the entity and general society. We further argue that specific barriers are often encountered in the data sharing process, effectively limiting the choices that supply chain participants have in making adequate data sharing decisions.

The remainder of this paper is structured as follows. Section II provides relevant background literature. Section III details the problem statement and the methodology applied in this research study. Sections IV and V present an overview of the exploratory results, whilst Section VI presents a detailed discussion on the outputs. Section VII concludes the study.

II. Background Literature

This section provides background literature concerning technology advances, privacy perceptions and attitude towards technology, specifically in the agri-food sector, and relevant advances in privacy preservation technologies.

A. Technology Advances

In modern-day business, entities are likely to be involved in multiple different supply chains and make use of technology systems, such as Intelligent agent technology, data mining, big data, cloud computing, IoT devices and RFID technology, to support the agricultural evolution [14] and achieving efficiency gains. According to Wiseman [23], Australian farms generate huge volumes of agricultural data, ranging from types of crops grown to crop yields, livestock numbers and locations, types

Workshop on Usable Security and Privacy (USEC) 2021
7 May 2021, Auckland, New Zealand
ISBN 1-891562-73-8
https://dx.doi.org/10.14722/usec.2021.23005
www.ndss-symposium.org

of fertilisers and pesticides used, soil types, rainfall and others. This data is typically collected using digital farming equipment with robotics, artificial intelligence, and IoT devices. These technology advances provide farmers with opportunities to manage their farms more efficiently, increase productivity and profitability, provide better management of risks and uncertainties and reduce the regulatory burden [13].

Integrated supply chain management offers advantages to individual supply chain participants, in particular by linking people and technology to better align the capabilities of each organisation and its trading partners [14]. This notion that technology can advance coordination amongst supply chain partners has been identified by various studies [2], [7], [21], although the cost and complexity of technological solutions remain some of the main barriers that discourage extended information sharing within supply chains [14]. Our study reveals a belief that industries can benefit from the flow-on effect from on-farm efficiency, supply chain optimisation, industry decision making, quality control and assurance.

B. Privacy Perceptions and Attitude Towards Technology

In other contexts, privacy concerns have been found to be a significant barrier to data sharing and re-use [6]. For example, despite the widely agreed benefits of data sharing and analytic platforms [5], these platforms carry the risk of illegally accessing, storing, sharing and potentially revealing private or confidential information about people and organisations. If not designed carefully, the information that should be protected may be released to the public, causing harm to farmers, damaging reputations and leading to legal infringements to platform providers.

Recent research into farmers' attitudes about sharing their farm data shows that about 60% of surveyed farmers have little to no trust in technology providers in maintaining their privacy and not engaging in unauthorised use of their data [5], [23]. Eurich et al. [8] find that *"the willingness to share data is lower the more expected negative consequences of potential risks are realized"*. Accordingly, trust and power are identified as important factors for data sharing, with companies preferring to share location information only with known, contracted partners. Their research states that *"the more power an organisation has with respect to its business partners, the lower the willingness to share will be."* Despite the relatively high level of distrust, statistics by *Successful Farming* [1] indicates that 70% of farmers are continuously using the internet on a daily basis and that farms are now, more than ever, embracing technology and closing the historical gap between rural and urban technology adoption.

Several researchers have studied this paradoxical behaviour [1], [16]. Acquisti et al. [1] find that people often have inaccurate perceptions of their own knowledge about privacy technology and vulnerabilities. Theoretical work around privacy often depict privacy perception and attitude towards technology as a trade-off or privacy paradox, where individuals exchange their private data for a service that is perceived as valuable. This privacy paradox refers to a *disconnect between an individual's preferred information sharing intentions and their actual disclosure practices*. The risk consequences influence behavioural intentions, but they are not strong enough to influence the actual disclosure behaviour, and therefore, attitude towards privacy is more conservative than the actual behaviour [24]. We find that although farmers are bracing technology in a bid to advance their farms and productivity, their perception of privacy is still a holding point in terms of data sharing within the supply chain.

[1]https://dkyinc.com/2017/12/how-farmers-are-using-digital-content-today-with-statistics

C. Privacy Preservation

The use of IoT has resulted in significant advancements in supply chains with the associated privacy concerns. *Identity privacy* concerns about people being unnecessarily identified when using a digital platform. E.g. registration details provided to the platform can be misused by other users or the platform's owner. *Location privacy* is concerned with the leakage of spatio-temporal preference information through the use of location information, including from smartphones [12]. The precise location of the source of food (e.g. cattle, crops requiring high water use) can expose farmers to the risk of being targeted by activists. These privacy issues can be mitigated using privacy preserving techniques.

For example, cryptographic techniques are used to prevent personal information leakage during transportation and in storage servers [4]; whereas anonymisation of users or using pseudonyms can help achieve privacy protection [15] and separate the location from the data [20]. Data aggregation approaches are used to provide summarised data instead of raw data, thereby removing identifiable information from the data [22], and data obfuscation can achieve privacy by transforming private data, for example, time or location, in such a way that the adversary cannot infer the data from other data [3]. Since a single mechanism might not be enough to ensure the protection of private information of the participants, a combination of these mechanisms can be useful [4].

III. Problem Statement and Methodology

In this section, we detail the problem that our exploratory research focuses on and present a detailed setup of our research approach.

A. Research Questions

Privacy is a fundamental human right that needs to be catered for, both in terms of physical privacy and privacy of personal information; even more so in an online environment. For our exploratory study, we consider that our target audience, suppliers in the food supply chain, often do not discriminate between the terms 'privacy' and 'confidentiality', and therefore, we consider these terms as interchangeable in this study.

Confidentiality and privacy are related to information with a scope beyond personal information. As highlighted by O'Hara [17], a person may feel comfortable to know that some information about them is known to friends, others to their banker and yet others to their doctor. However, the person may not feel comfortable in either of the three knowing all information about them. The reason is that the collection of information about an individual allows extraction of knowledge about the individual's habits, beliefs and health and therefore may create an unfair disadvantage to the individual [19].

Similarly, organisations may be comfortable in sharing some information with their suppliers, others with their clients and some more with their governing bodies. However, they may not be comfortable sharing all the information with everyone. Therefore, we need to consider both personal and organisational privacy in supply chain application platforms. Within our specific target audience, there is no clear delineation between personal and organisational privacy, particularly in the case of farmers where their personal profiles are largely linked with their organisational profiles. Accordingly, we do not differentiate specifically between these privacy domains.

In this research, we postulate that people are constrained by specific situations when making privacy related decisions, and that their privacy perception is therefore duly influenced. In support of this postulation, we focus on two specific research questions:

- **Research question 1:** What are the perceived benefits and risks in sharing data from the supply chain participant's viewpoint?
- **Research question 2:** How do these perceptions match the assumptions of research in privacy preserving transformations?

B. Research Methodology

Our exploratory research focuses on the perception of trade-off between individuals' privacy concerns and the value obtained by the supply chain as a whole. This theoretical postulation is supported by two small-scale observational studies to refine the perceived social and technical barriers in terms of data sharing and privacy. We applied a research instrument with interviews and questionnaires to supplement the traditionally low response rate expected from questionnaires sent to a non-individualised target group.

1) Interviews - A: We first conducted four independent *interviews with industry-level stakeholders* in Australia. An invitation to participate in these interviews was sent in November and December 2018 to a number of industry-level stakeholders across the wider scope of the supply chain. We specifically approached stakeholders that could provide us with insights into the broader food supply chain industry. The participants who accepted our invitations included[2],

- A CEO of an ICT peak body
- A Director of a food sector peak body
- A Manager of a food producer
- An Associate Director of a consulting company specialising in supply chain issues

The interviews were open ended with provoking questions including:

- What opportunities and risks arise with the move towards greater data sharing (for the purposes of understanding food quality and provenance) across supply chains in Australia's food industry?
- Who do you see as the main beneficiaries of data sharing initiatives in the food industry and why?
- Do you think there will be any groups or participants in the food industry who could be disadvantaged with greater data sharing across food supply chains and if so, how?
- What regulatory arrangements, policies, information or resources will be needed to appropriately manage the opportunities and risks surrounding data sharing for food provenance?
- Do you have any views on whether certain types of data are more or less appropriate for data sharing for the purpose of understanding food provenance?

All interviews were audio-recorded and transcribed. Verbal consents were obtained before the start of the interviews.

2) Interviews - B: Following the first set of interviews, we initially investigated the option to run the online questionnaire through an online survey panel that specialises in obtaining quality targeted participant responses. However, the specificity of our targeted audience was not viable with the available audience pool. As such, we relied on practical interactions and word-of-mouth advertising and recommendations of our survey and interviews. Consequently, our invitation to participate through either the online questionnaire or the second set of interviews was shared in July 2019 through several associations in the food sector and remained open for 9 weeks. Among the responses, only four *farmers and other individual supply chain participants* accepted our invitation for the interview. The interview questions included:

- What are the current information sharing practices in your supply chain?
- What do you think about data analytics platforms? (examples of data analytics were verbally provided during the interviews)
- What do you think about privacy preserving technologies? (brief information about privacy preserving technologies was verbally provided before asking this question)
- How do you learn about new technologies and developments?

These interviews were also audio recorded and transcribed, and verbal consents were obtained before the interviews.

3) Questionnaire: Finally, we conducted an interactive *online questionnaire with farmers and other supply chain participants*. These questions were adapted from the second interview's questions to be suitable to a broader audience through the online platform. The design of the survey instrument included mapping the research questions to Likert scaled questions to be asked, and including scenario-based questions aimed at extracting realistic behaviour and validated perceptions. Questions to capture participant characteristics (part of the food sector, geography, experience) were also included. The questions were formulated to gain insight into the perceived importance and risks of data sharing practices and the perception of privacy preserving techniques in this non-traditional usable security user group. The online questionnaire was hosted through SurveyMonkey[3] and was completed digitally by participants.

[2]We provide organisational identities at a very high level to protect participants' identities.

[3]https://www.surveymonkey.com/

Since the invitation was sent through the industry associations, the exact number of invitations circulated were not known but estimated to be approximately 4000. In addition, participants were actively recruited by approaching stallholders at two Farmer's Markets (Capital Region Farmers Market and Southside Farmers Market in Australian Capital Territory) and two Fresh Food Markets (Belconnen and Fyshwick) in Canberra, Australia. These locations were chosen for the researchers' convenience. During active recruitment, participants were provided with the technical means (an iPad with a mobile data connection to SurveyMonkey) to complete the questionnaire whilst tending to their stalls.

All studies were approved by the CSIRO ethics review board. Prior to its dissemination, all question sets were pilot tested with two researchers in the Agriculture and Food environment to uncover any ambiguities and ensure that the questionnaire could be completed in a reasonable time.

C. Sample Statistics

The data collection was subjective in nature, collecting both facts and opinions of the participants on the subject area in a closed-ended design. Table I shows the summary of our study samples, and Table II shows the participants' characteristics for the online questionnaire.

TABLE I. PARTICIPANT SUMMARY

Interviews - A	4 Executive level officers
Interviews - B	4 Farmers and food supply chain participants
Questionnaire	51 participants (out of approx 4000 invitations) - two incomplete responses removed

TABLE II. ONLINE QUESTIONNAIRE PARTICIPANT CHARACTERISTICS

Ower/Manager	88%
Experience (10-15 years)	20%
Experience (15+ years)	49%

Despite the low response rate, we believe that our participants provided a reasonable representation of the views of the population within the domain.

D. Study Limitations

The purpose of this research study is to explore people's stated attitudes to privacy and the reasoning behind their decision process. However, the subsequent findings discussed in the next section are limited to the scope, and participant representation of this study, and readers are cautioned when interpreting the generalised findings.

1) Narrow Scope: An important consideration in this research is that individual's privacy perceptions and their associated privacy concerns are influenced by their own personal and professional experiences, their understanding of technological innovations and their position within a given supply chain. All of these aspects contribute to the creation and identification of perceived constraints within the choices that the individuals make in terms of privacy. This very narrow project scope limited the participant from primary industry supply chain stakeholders, with specific emphasis on roleplayers in the farming and processing parts of the agriculture supply chain.

2) Non-representative Samples: Given the nature of the target audience, it was very difficult to attract a good and representative range of participants. Therefore, our study was conducted with a small group of targeted stakeholders, and may not definitively represent the primary industry supply chain stakeholders. The survey results are applied as supplementary data to support the theoretical foundation of this research study and to provide a base understanding in terms of privacy trade off and technology adoption. The insights from the survey are not taken as indicative or representative.

In the next section, we report a selection of the most relevant results from our observational studies. We discuss the major findings of the study related to privacy trade-off. We further consider findings in terms of data sharing and trust-building.

IV. PRIVACY TRADE OFF IN SUPPLY CHAINS

This section addresses the main challenge of the research and presents information to address the first research question, with specific relevance to privacy trade-off: *What are the perceived benefits and risks in sharing data from the supply chain participant's viewpoint?* To understand the perception of supply chain participants, we establish their current view on information sharing practices and then investigate more in-depth to establish the perceived benefits thereof.

A. Current Information Sharing Practices

In understanding the depth of privacy trade-off within the supply chain, we formed a baseline of food supply chain participants' current practices and attitudes towards information sharing, both upstream (to their suppliers) and downstream (to their clients). In identifying these data sharing practices, we specifically excluded data sharing attitude regarding financial transaction related information, but instead focused on additional information that could be shared, such as requirements specifications, information about processes or stock levels. Questions that we asked both interview and questionnaire participants include:

- Do you currently share any information with your suppliers (i.e. upstream)?
- What type(s) of information do you share with your suppliers? (options provided as listed in Fig. 2)
- Do you currently share any information with your clients (i.e. downstream)?
- What type(s) of information do you share with your clients? (options provided as listed in Fig. 2)
- Are you required (e.g. through regulation, contract) to share information?

In terms of **downstream information sharing**, we found that 96% of participants indicated that they share production specifications, followed by 63% that stated that they share information with suppliers, such as production information received from the supplier. 61% of participants indicated that they share processes, and 59% responded that they share information about their suppliers. 27% of participants revealed that they share stock levels. The majority of questionnaire participants share additional information with their clients,

despite this not being a strict requirement enforced by law, industry or the client. This trend is present with both sets of interviewees. Interview participants concurred that downstream sharing is more common with consumable products where consumers would be concerned about ingesting a good quality product at the end of the supply chain, such as beef or eggs. It is less prevalent with non-ingested by-products, such as wool. For example, a farmer working with livestock provided specific information about the animals (age, condition, vaccines received, etc.) and declared which chemicals were given to particular animals and at what point in their life. This information travelled with the animals all the way to the abattoirs. Similarly, in the case of a farmer working with produce, a complete record needed to be kept of how and what sort of crops were raised, how much water was used for irrigation, how many weeds were present, etc. This information travelled with the produce along its lifecycle.

Upstream information sharing occurs at a lesser extent and is more focused on feedback. 51% of questionnaire participants indicated that they share requirements specifications, followed by 35% that share information from customers, such as feedback and information requests received. 25% of questionnaire participants declared sharing of stock levels and 20% of participants indicated sharing of processes. Feedback obtained from the interviews shows that upstream information sharing is often very basic. We found interview and questionnaire participants split equally in terms of sharing/not sharing information with their suppliers. All participants indicated that they share information voluntarily; it is not an enforced requirement but instead done to affect the warranties. Upstream information sharing was primarily related to negative feedback such as product-specification mismatch. For example, an animal farmer expects to receive feedback only when the animal does not meet product specification. Similarly, if a batch of seed does not germinate or the farmer witnesses an adverse effect of the veterinary medicines, this would be reported to the supplier. Interviewee 2-1 stated it simply:

> I buy a product, [if] it works, I don't bother to tell anyone ... I keep using the product ... if it doesn't work, then I complain, and often the producer will ... replace or in some way or another make it good for me.

B. Perceived Benefits and Disadvantages of Information Sharing Practices

The benefits perceived by stakeholders in the food supply chain is a personal matter, with individuals' own experiences, circumstances and understanding of the technology involved heavily influencing their evaluation of the perceived benefits. To understand the perceived benefits of the current information sharing practices detailed in Section IV-A, we included a scenario in our questions referring to a platform that can store and analyse supply chain data to explore participants' privacy perceptions. This platform would allow analytics such as forecasting and reporting of a participant's data combined with other data. Questions that we asked both interview and questionnaire participants were:

- Would you consider (or are you already) using a supply chain analytics platform?
- *If yes*,
  - What type(s) of information would you be comfortable providing to such a platform (options provided as listed in Fig. 2)
  - What type of information would you like to get from such a platform? (options include 'analytics', 'aggregated map views', 'demand/market forecasting' and 'other')
- *If no*, Why wouldn't you consider using such a platform?

Fig. 1 shows questionnaire participants' attitude towards such a supply chain analytics platform, with blue responses reflecting those currently not sharing or intending to share data and red responses reflecting those currently sharing or considering sharing data via a supply chain analytics platform. These responses are mapped to the participant responses on sharing information with clients in Section IV-A. Among the participants, a smaller number of participants were either already using or intended to use a supply chain analytics platform, in comparison with participants that were not currently using or intending to use such a platform in the near future. Interestingly, about half of the participants who indicated that they did not share any information with their clients, also mentioned that they were using or intent to use in the near future a supply chain analytics platform suggesting that the participants had a disconnected perception between the use of a digital platform and information sharing.

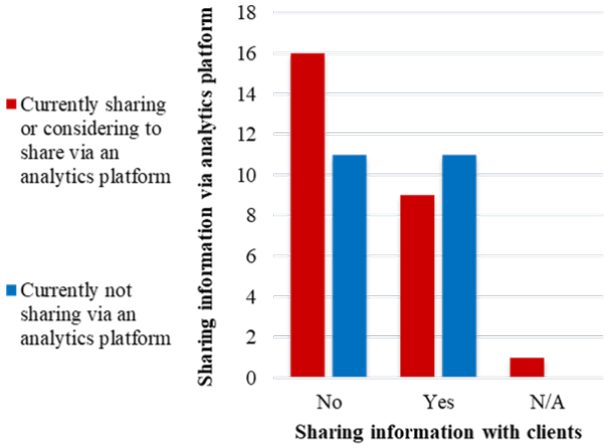

Fig. 1. Attitude towards supply chain analytics platform mapped to sharing of information with clients

Fig. 2 looks particularly at the information types that questionnaire participants indicated they would be comfortable to share with such a platform. Participants are most likely to share information on production specifications and less likely to share information regarding stock levels due to the potential commercial sensitivity thereof. All other information are fairly consistently indicated as possible information to be shared. Participants indicated that they would be comfortable to receive analytics, demand/market forecasts and aggregated map views from such a supply chain analytics platform. In most cases, participants that indicated a positive attitude towards a supply chain analytics platform are only slightly more than those that indicated a negative attitude.

The interviews provided many qualitative views on the benefits of using a supply chain analytics platform. When asked during the interviews who would benefit the most as

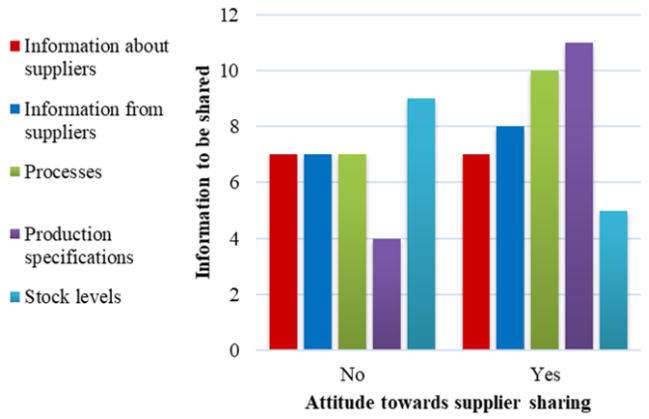

Fig. 2. Attitude towards supply chain analytics platform mapped to shared information types

a result of data sharing, a more nuanced view emerged. The view was that the benefits of data sharing would vary according to the type of data being shared, who had the knowledge and expertise to analyse and interpret the data, and what type of food product was involved. E.g. producers who were offering a premium or highly perishable product were more likely to benefit from data sharing than producers of more commoditised products. Interviewee 1-2 considered provenance as most important:

> For a consumer to know that something is safe, is important... So I think data sharing is important... it enables you to tell your story better because people see data as more solid evidence rather than just saying.

Interviewee 1-3 shared a specific scenario in instances where food contamination occurs, where authorities would be able to respond more quickly by tracing the problem to its source and determining the most appropriate mitigation strategy. Interviewee 1-4 remarked on the potential reduction in worker exploitation in the horticultural sector by making labour practices more transparent with a data sharing platform. Particularly, the value of such a platform was seen in benchmarking against other organisations in the same industry.

When asked who might be disadvantaged as a result of greater data sharing in food supply chains, three groups were identified. First, participants in the supply chain who were engaged in suboptimal practices would be disadvantaged, since data sharing should help to expose these practices. Second, data owners could be disadvantaged if they bear the cost of providing the data without receiving a benefit from sharing their data. Third, greater data sharing could potentially reduce the advantage that retailers have currently since retailers currently have more access to data than other participants in the Australian food supply chains. Interviewee 1-1 explained:

> There is the risk... for the big end of town to have the resources available to them to take more advantage of the data ahead of the smaller players... The smaller players actually have far more agility to be able to respond to opportunities than what the larger players do by making as much data open and equally accessible by as many players as possible, is of benefit to the ecosystem because then it, kind of, levels the playing field in that regard.

Interviewee 1-3 added the following context:

> The first people [disadvantaged] would be retailers because they have greater insight than any other sector so if for some reason if data sharing was encouraged on a commercial basis a bit further up the supply chain then there might be retailers that might get less value out of it.

One participant acknowledged that there was potential for consumers' and organisations' interests to conflict and that it would be important to consider when there is a real benefit, who benefits and what the downside of data sharing might be. Trust from the consumer perspective was highly regarded by the participants, particularly focusing on the consumer's trust that the product is safe. Interviewee 1-2 stated clearly that ownership and transparency in terms of control is an important factor. Some of the participants indicated that previous failed attempts to use such a data sharing platform had a negative impact on their trust in such technologies.

Although many participants do not currently share information with their clients, they see the potential benefit that sharing specific information would bring. We, therefore, make the assumption that if all the participants' concerns regarding the analytics information sharing platform are sufficiently addressed, they would be more likely to support this.

V. Building Trust in Data Sharing

This section provides additional information in addressing the first research question, with specific relevance to adapting privacy perception in data sharing practices. It further addresses the second research question: *How do these perceptions match the assumptions of work in privacy preserving transformations?* To understand how the privacy perception of supply chain participants maps against privacy preserving transformations, we consider the trust factor in data sharing.

A. Privacy Preserving Technology

In the traditional functioning of a supply chain, participants receive material from their providers and sell goods to their customers, thereby creating a supply chain for primary produce from farmers to processors to distributors to retailers. Each supply chain entity has personal and/or commercial sensitive information and the sharing of such data with others could create a risk of data being misused. For example, a dairy farmer has sensitive information such as volume sold, prices, precise locations and exact times when selling and buying events occur. We introduced the concept of privacy preserving technology across supply chains within our interview scripts and online questionnaire and tested the participants' attitudes towards such technology to address some of the privacy concerns raised in Section IV. In our scenario, privacy preserving technology can ensure that sensitive information is not available to others, although high-level information, such as general forecasts, would be available. Questions that we asked both interview and questionnaire participants include:

- How useful would such a supply chain analytics platform be in your supply chain? (5-point rating between 'useless' and 'very useful')
- How trustworthy would you regard such a technology for preserving your confidential information? (5-point rating between 'untrustworthy' and 'very trustworthy')

- If the comprehensive software platform for supply chains is built using privacy preserving technologies, how likely is it that you will consider using the platform? (5-point rating between 'unlikely' and 'very likely')
- If the comprehensive software platform for supply chains allows you to control and monitor the use of your data, how comfortable would you feel using the platform? (5-point rating between 'uncomfortable' and 'very comfortable')

We found that 49% of questionnaire participants regarded privacy preserving technologies as somewhat useful. 29% of questionnaire participants indicated that they regard privacy preserving technologies as very useful, despite more than half of them not showing support for the platform. 33% of questionnaire participants indicated that such a technology would be somewhat trustworthy, whilst a further 33% indicated that such a platform would be completely untrustworthy. There is a very clear divide in participants that see the value in such technology, both in terms of usefulness and trustworthiness.

In exploring questionnaire participants' attitude towards using the supply chain analytics platform if privacy preserving technologies were built in, 31% of participants indicated that they are somewhat likely, and 14% of participants indicating that they are very likely to use the privacy preserving technology based platform. 29% of participants indicated that they are very unlikely to use the platform even with the addition of privacy preserving technologies. If given the opportunity to control and monitor their own data, we found that 39% of the participants indicated that they would be somewhat comfortable with using the platform. An additional 20% of participants indicated that they are very comfortable to use the platform. This is in contrast to 18% of participants that indicated that they are uncomfortable, and 10% of participants indicating that they are somewhat uncomfortable to use the platform, even with the additional data control.

The Sankey diagram in Fig. 3 shows the proportional flow in participant responses from one question to the next, with the five questions displayed on the x-axis and the participant numbers on the y-axis. The dark vertical bars corresponding with the questions reflect the participants' ++ (very positive), + (positive), 0 (neutral), - (negative) and - - (very negative) responses. From this diagram, we found that over 50% of participants responded that they would not join the initially proposed data sharing platform (- - in the purple vertical bar), although many of these participants indicated that privacy preserving technologies would be considered quite useful (+ and ++ in the blue vertical bar). The trust in privacy preserving technologies (orange vertical bar) is quite balanced, and so is the willingness to join the platform, if it would be based on privacy preserving technologies (pink vertical bar). If they could monitor and control the use of their data, the majority of participants would feel comfortable using the platform (+ and ++ in the green vertical bar). Our results show a clear trade-off between data usage and privacy risk, while transparency and the ability to control clearly improve comfort in using the platform.

The participants in the interviews showed a mixed response in terms of the addition of privacy preserving technologies. The possibility of technology that might fail was a major consideration. They were concerned about the legal implication that would arise from technology failure and the possibility to trace back information to a specific entity.

B. Intention to Use / Technology Adoption

Our preliminary investigation shows that participants are impartial to using a data analytics platform, and the addition of privacy preserving mechanisms did not lead to more a predominate intention to adopt the technology. Some concerns were raised in terms of scope and boundaries of such a platform, with particular concerns that other organisations would know the level of success or failure. Participants also identified key risks that would need to be managed, relating to the accuracy and interpretability of data being shared and the potential for loss of intellectual property and privacy. Participants were in agreement that effort needed to be directed towards ensuring that the system could be trusted, especially where data were used to address food safety concerns.

With regard to digital data sharing, we observed some awareness of problems with cloud-based platforms, with data breaches regularly in the news, and erosion of trust as some organisations used users' data for their own benefit. These issues need to be addressed to regain confidence in organisations and that they can be trusted to protect the users' data. Interviewee 1-1 also specifically raised the cyber security concern:

> For example, if data was put into that shared arrangement that provided... authentication to the fact that there were no allergens in the food... but in fact that data had been messed with to say that there aren't any allergens when there actually are, that's playing with lives.

In terms of prediction and forecasting, it was clear that the interviewees are more inclined to trust their own instincts and experiences. Interviewee 2-2 stated:

> Oh, I wouldn't believe their forecasts... I know on my own when I sell wheat or lambs or anything else, that I pick my time to sell it. I know [based on] past years what the highest price will be at the certain time of the year.

Based on both the interviews and the online questionnaire, we find that supply chain stakeholders have a very clear idea of what aspects of a data sharing platform would have to be addressed in order for their trust to be acknowledged. The benefits identified weigh strongly and serve to sway stakeholders to a general acceptance, but the unknown details and repercussions of technology advances and the ultimate need to maintain secure and competitive remains.

VI. Discussion and Recommendation

A supply chain consists of several participants with different interests and perceptions, making data sharing among participants complicated. Despite significant growth and innovation acceleration, digital agriculture is in an immature state in many aspects [5] and many participants are not easily adapting to online security and trust. We presented results from our exploratory study, through two sets of qualitative interviews and an online questionnaire. Fig. 4 provides an overview of our findings.

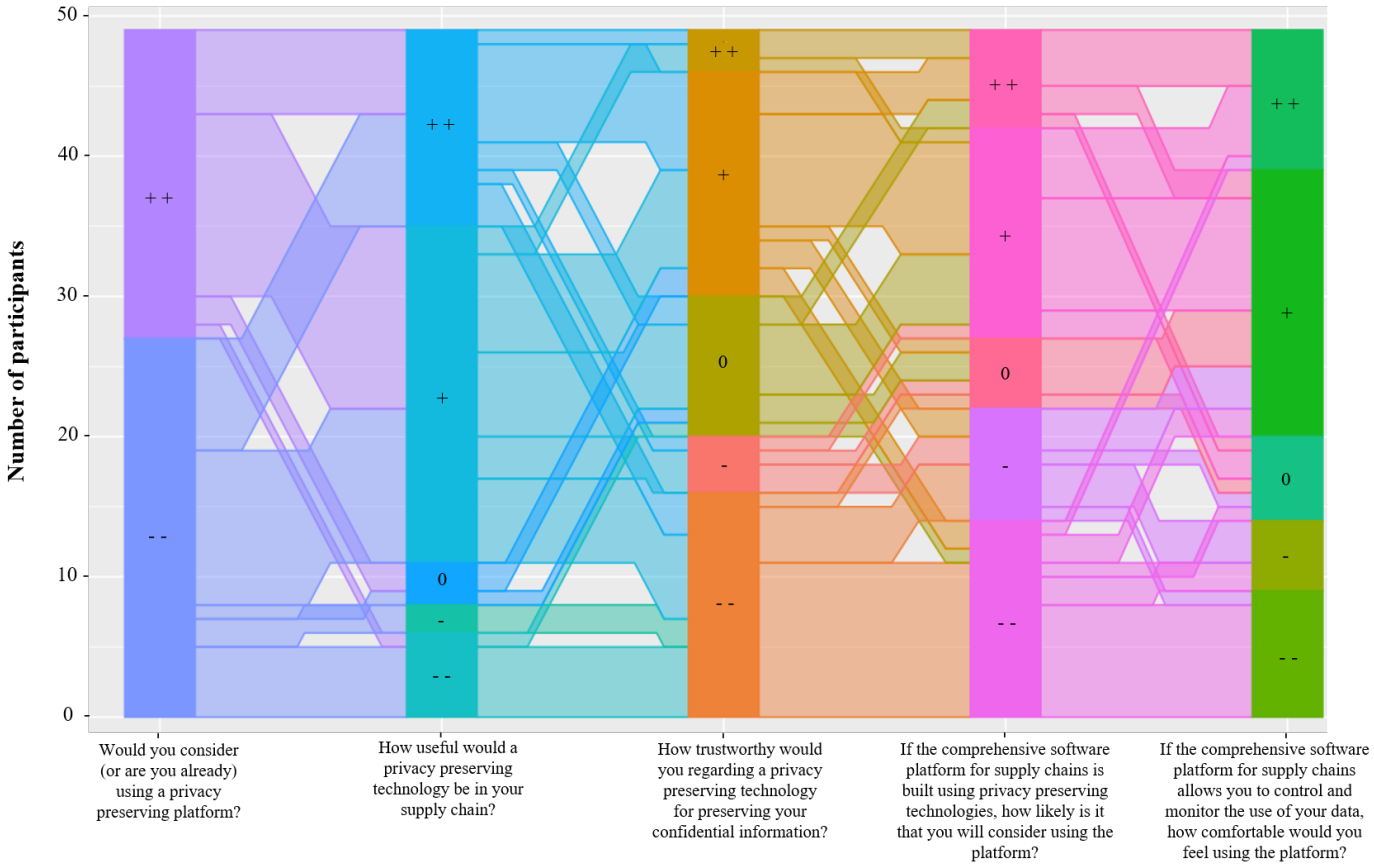

Fig. 3. Distribution of responses over different survey questions

A. *Research Question 1*

We specifically investigated what the perceived benefits and risks are in data sharing from the viewpoint of the food supply chain participants. We further identified several social and technical barriers that could introduce structural constraints in the choice of decisions that supply chain participants can make, and counter the adoption of usable security in the food supply chain.

(1) Inconsistent views exist on perceived benefits and risks of data sharing technologies. In the first interview set, we looked at the privacy and confidentiality issues in the supply chain. Our interviews with high-level authorities and stakeholders showed that they focus on the big picture, and perceive more benefits than risks of data sharing in the supply chain. They identified several benefits as well as barriers and risks of data sharing. However, in the second interview set, we found that producers/farmers are often not interested in sharing data mainly because they do not perceive getting enough value from this. The most likely risk in adopting a data sharing analytics platforms would be an unbalanced adoption of such technology without all participants onboard.

(2) There is an asymmetry in the willingness of data sharing upstream and downstream in a supply chain, similar to findings in a previous study [10]. People generally do not provide positive feedback and are more inclined to provide negative feedback if they are not satisfied with a service or product. Even when supply chain participants recognise some benefit, they still remain uninterested due to the perceived effort required to process the data. When the value and benefits are significant, some people do not trust others having their data due to risks of losing organisational confidentiality and privacy leading to negative consequences. Many individuals are unwilling to share information that they perceive may place their organisations at a competitive disadvantage. Such asymmetry raises questions about an organisation's openness and willingness to share information honestly and frequently, which determines the extent and quality of data shared [9].

(3) People have an ambiguous distinction between privacy and confidentiality. Agricultural data is often connected to farmers' personal information. For example, the location of the farms or GPS-enabled farming equipment may be digitally linked to farmers' names and financial information. Within industries, anecdotal stories abound about banks and insurance companies knowing more about the incomes and management of farms than the individual farmers themselves [23]. Accordingly, we noticed that the terms privacy and confidentiality are used ambiguously by different participants. In the context of privacy law, the meaning of privacy is focused on data about individuals, whereas the term privacy is sometimes used to mean much more than the personal data, including information at the organisational level.

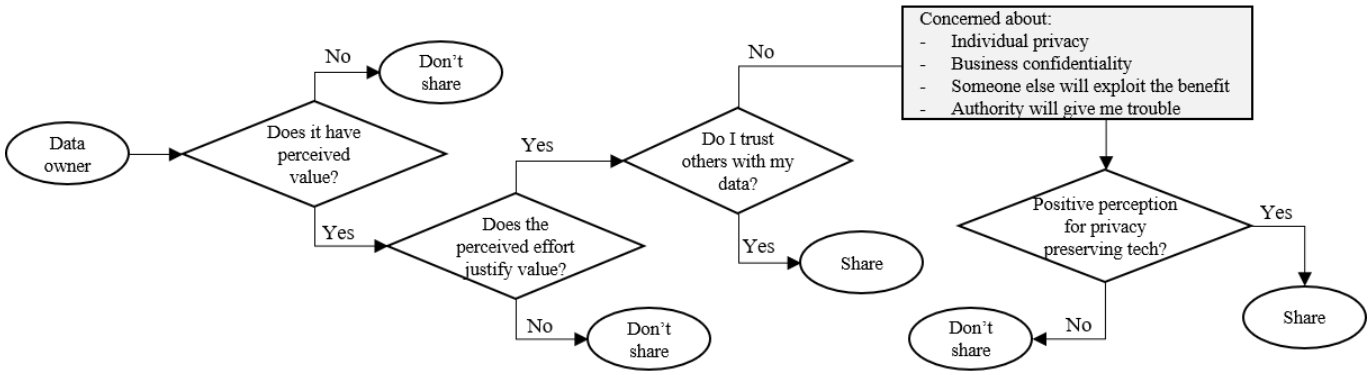

Fig. 4. Data sharing barriers working against usable security

B. Research Question 2

We further investigated how the perceived benefits and risk in data sharing match the assumption of privacy preserving transformations. Although our results show a slight increase in people's inclination to sharing data when privacy preserving transformations are applied, this result might have two limitations. First, based on Fig. 4, most of the negative results could be driven by stakeholders' current share/don't share position. For example, those who might have seen the value in the current practices were more inclined to share data when privacy preserving technologies were used. Second, those who did not perceive value in such a system, or who thought that the new system would create a lot of extra work burden to them were indifferent to technology.

Therefore, **(4) trust and power are important factors for data sharing**. Our participants raised concerns that others (competitors and non-competitors) could be reaping more benefits than themselves. Privacy preserving technologies are perceived as having a positive impact on people who see value in sharing data and who trust others with their data, but have concerns about organisational confidentiality and privacy. It was clear that the way in which the cost of infrastructure for data sharing and providing data sharing need to be managed in a way to allow all participants to benefit.

(5) Users prefer more visibility and control over the collection, aggregation and potential distribution of that data. Data sharing, which would improve the connection between the food producer and consumer, would make it easier for Australian producers to identify gaps in the market, market themselves and establish useful partnerships, reduce fraud and command a premium for their product (by demonstrating its provenance). In fact, data sharing is expected to increase producers' share of the global food market because of Australia's reputation for producing high quality and safe food products. However, in reality, the integration of technology and advanced systems enable modern farms to create a large amount of data, but farmers have little control over it. We, therefore, ascertain that farmers and their direct stakeholders are aware of the changing data landscape. Still, matters related to privacy, confidentiality, visibility and control are not perceived equally amongst them, causing a break in optimal data sharing that could benefit the entire supply chain.

(6) The privacy paradox has implications for the design of privacy systems. Previous work on privacy has identified that individuals make privacy decisions as part of a privacy trade-off, exchanging data for services of value. However, it has also shown that behaviour is often not consistent with people's stated privacy values, i.e. *the privacy paradox*. People actually acting differently than their stated preferences imply [24] was also observed in our study. In terms of privacy preserving technology, it is essential to realise that shared data may hold very sensitive personal information and that a privacy preserving supply analytics platform need to be fully secured. As such, specific care needs to be taken by designers of data analytics platforms to remediate the gap between stated privacy values and privacy behaviour, expand the availability of research, increase transparency and enable reproducibility [6]. The platform needs to be designed to cover all aspects of the supply chain, in particular the user (covering all users of the system, from non-tech savvy individuals to clued up cyber experts), usage (ranging from basic data sharing to advance benchmarking and forecasting) and usability aspects (intuitive and self-adaptive) as discussed in our previous work in a similar context [11].

VII. Conclusion

While data sharing could enhance the efficiencies of food supply chains, privacy and confidentiality of shared information have been considered as a primary concern, and the application of privacy preserving technologies is expected to address those concerns. However, improving trust in such data sharing applications requires us to understand the participant's perception towards such technologies. This exploratory study was conducted to understand those perceptions. The results and implications are limited by the scope and sample size of this study, and further research may help to draw more precise and accurate conclusions.

Because data collection and sharing in the agriculture domain involve personal information that can directly be linked to the livelihood of the farmers, privacy perceptions and attitude to technology adoption is not straightforward [6]. Across two sets of exploratory qualitative interviews and an online questionnaire, we found a distinct divide in terms of perceived benefits and risks associated with a data sharing platform, as well as the perceived protection offered through the addition of privacy preserving technologies. Although many different stakeholders across the supply chain have a fair interpretation

of the benefits that such a platform would bring, the individual farmers recognised significantly more risks, and a disparity between efforts required from them and the benefits they may received. There is a clear divide between participants; some participants see the value in analytic technology platforms in terms of usefulness and trustworthiness, yet do not consider them as a data sharing platform, while other participants are more sceptic in terms of the perceived value of the platform.

Our study has three key implications for data sharing platform developers and policy makers for food supply chains. Firstly, current data sharing practices between upstream and downstream are asymmetrical. Also, the perceptions of the flow of benefits and efforts required are not uniform. Therefore, greater adaption of a data sharing platform will need better clarity on the cost/benefits for each supply chain participant. Ensuring a flow of value towards upstream participants may further help reduce the barriers of adaption. Secondly, supply chain participants, particularly those whose competitive advantage depends on data, need more visibility and control over the use of their data. Since privacy preserving technologies can help improve trust, the providers may need to educate their users about how such technologies are used and how the sensitivity is reduced from their data. To increase the trust of users in IoT applications and systems, and thereby pave the way for broader adaption, security and privacy protection solutions should also involve and support users in the protection of their data and privacy, i.e., users should be supported to understand how their data is collected, processed, analysed, stored, accessed and kept safe. Thirdly, supply chain participants can have a disconnect between their beliefs and actions. Therefore, platform providers need to be careful when observing and interpreting the needs of their potential users. Explicitly clarifying their needs and understanding their best interest may help improve the trustworthiness of such platforms.

REFERENCES

[1] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015. [Online]. Available: https://science.sciencemag.org/content/347/6221/509

[2] A. Ajay and M. Maharaj, "Effects of information sharing within supply chains," *Proceedings of the Southern African Computer Lecturers' Association (SACLA) 2010*, pp. 35–42, Jun 2010.

[3] D. Bakken, R. Rarameswaran, D. Blough, A. Franz, and T. Palmer, "Data obfuscation: Anonymity and desensitization of usable data sets," *IEEE Security & Privacy*, vol. 2, no. 6, pp. 34–41, 2004.

[4] S. Blasco, J. Bustos-Jiménez, G. Font, A. Hevia, and M. Prato, "A three-layer approach for protecting smart-citizens privacy in crowdsensing projects," *IEEE SCCC*, 2015. [Online]. Available: http://dblp.org/rec/conf/sccc/BlascoBFHP15

[5] Cotton Research and Development Corporation (CRDC). (2020) "Accelerating precision to decision agriculture". May 29, 2020. [Online]. Available: https://www.crdc.com.au/precision-to-decision

[6] R. Curty, A. Yoon, W. Jeng, and J. Qin, "Untangling data sharing and reuse in social sciences," *ASIST '16: Proceedings of the 79th ASIS&T Annual Meeting: Creating Knowledge, Enhancing Lives through Information & Technology*, no. 25, pp. 1–5, October 2016. [Online]. Available: https://dl.acm.org/doi/abs/10.5555/3017447.3017472

[7] S. Dong, S. Xu, and K. Zhu, "Information technology in supply chains: The value of it-enabled resources under competition," *Information Technology in Supply Chains Information Systems Research*, vol. 20, no. 1, pp. 18–32, 2009.

[8] M. Eurich, N. Oertel, and R. Boutellier, "The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain," *Electronic Commerce Research*, vol. 10, no. 3, pp. 423–440, 2010.

[9] S. Fawcett, P. Osterhaus, G. Magnan, J. Brau, and M. McCarter, "Information sharing and supply chain performance: The role of connectivity and willingness," *Supply Chain Management: An International Journal*, vol. 12, no. 5, pp. 358–368, 2007.

[10] P. Fiala, "Information sharing in supply chains," *Omega*, vol. 33, pp. 419–423, Jun 2005. [Online]. Available: https://doi.org/10.1016/j.omega.2004.07.006

[11] M. Grobler, R. Gaire, and S. Nepal, "User, usage and usability: Redefining human centric cyber security," *Frontiers in Big Data*, vol. 4, p. 5, 2021.

[12] J. Hamm, Y. Cao, and M. Belkin, "Learning privately from multiparty data," in *Proceedings of The 33rd International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, M. F. Balcan and K. Q. Weinberger, Eds., vol. 48. New York, New York, USA: PMLR, 20–22 Jun 2016, pp. 555–563. [Online]. Available: http://proceedings.mlr.press/v48/hamm16.html

[13] E. Jakku, B. Taylor, A. Fleming, C. Mason, and P. Thorburn, "Big data, trust and collaboration: Exploring the socio-technical enabling conditions for big data in the grains industry," CSIRO Agriculter and Land & Water, Brisbane, Australia, Tech. Rep., 2016. [Online]. Available: https://publications.csiro.au/rpr/download?pid=csiro:EP164134&dsid=DS2

[14] C. Marinagi, C. Skourlas, and E. Galiotou, "Advanced information technology solutions for implementing information sharing across supply chains," *PCI '18: Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, pp. 99–102, November 2018, https://dl.acm.org/doi/pdf/10.1145/3291533.3291575.

[15] A. Martinez-Balleste, P. Perez-Martinez, and A. Solanas, "The pursuit of citizens? privacy: A privacy-aware smart city is possible," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 136–141, 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6525606/

[16] M. Mattevi and J. Jones, "Food supply chain: Are UK small to medium sized enterprises (SME) aware of concept, drivers, benefits & barriers, and frameworks of traceability?" *British Food Journal*, vol. 118, no. 5, pp. 1107–1128, 2016.

[17] K. O'Hara, "Transparent government, not transparent citizens: A report on privacy and transparency for the Cabinet Office," the University of Southampton, Tech. Rep., September 2011, Cabinet Office.

[18] H. Sarjono, B. Jadi, and B. Handoko, "Supply chain for potato products in Tawangmangu, Central Java, Indonesia," *ICEME 2019: Proceedings of the 2019 10th International Conference on E-business, Management and Economics*, pp. 274–278, July 2019.

[19] D. J. Solove, "Why privacy matters even if you have 'nothing to hide'," *Chronicle of Higher Education*, vol. 15, 2011.

[20] H. To and C. Shahabi, *Location Privacy in Spatial Crowdsourcing*. Cham: Springer International Publishing, 2018, pp. 167–194.

[21] M. Torabizadeh, M. Khatami Rad, and A. Noshadi, "Effect of information system strategies on supply chain strategies and supply chain performance," *World Academy of Science, Engineering and Technology*, vol. 61, pp. 940–945, 2012.

[22] I. Vakilinia, J. Xin, M. Li, and L. Guo, "Privacy-preserving data aggregation over incomplete data for crowdsensing," *GLOBECOM*, 2016. [Online]. Available: http://dblp.org/rec/conf/globecom/VakiliniaXLG16

[23] L. Wiseman and J. Sanderson. (2019) "farmers create lots of data, but farmers don't control where it ends up and who can use it". April 16, 2019. [Online]. Available: https://theconversation.com/farms-create-lots-of-data-but-farmers-dont-control-where-it-ends-up-and-who-can-use-it-115228

[24] A. Zafeiropoulou, D. Millard, C. Webber, and K. O'Hara, "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?" *WebSci '13: Proceedings of the 5th Annual ACM Web Science Conference*, pp. 463–472, 2013.