© The Author 2022. Published by Oxford University Press on behalf of The British Computer Society. All rights reserved.
For Permissions, please email: journals.permissions@oup.com
doi:10.1093/iwcomp/xxxxxx

Participatory Data Design: Managing Data Sovereignty in IoT Solutions

Judy Bowen and Annika Hinze

The University of Waikato, Hamilton, New Zealand

Within the software engineering community, deciding how to collect, store and use personal data has become about more than just understanding our users. This paper considers ethical data use which includes cultural considerations and data ownership rights. We discuss indigenous data sovereignty as a concept and how it potentially impacts technological solutions that gather personal data from users. We propose an extension to typical user-centred design processes which we call participatory data design. This incorporates the use of frameworks and tools that specifically focus on managing data within the cultural context it is gathered from. We also present a specific example of how we have used this approach in the context of a data collection project from Māori workers in New Zealand forestry. We conclude with a discussion of the wider implications of this approach.

Keywords: software development methods; indigenous data sovereignty; Internet of Things; personal data; cultural perspectives

1. RESEARCH HIGHLIGHTS

- A discussion of cultural data considerations within IoT.
- An extension to the classic participatory engineering design process which enables consideration of indigenous data sovereignty.
- Description of practical application of the process described within the context of New Zealand.

2. INTRODUCTION

Large-scale "Internet of Things" (IoT) solutions aimed at smart-homes, smart-cities and smart-environments are regularly proposed as envisaged futures. Current academic research focuses on quality criteria for IoT solutions, such as security (Zhang and Green, 2015; Grammatikis et al., 2019), data privacy (Bertino, 2017) and robust connectivity (Sarkar, 2016). Here, however, we consider issues of IoT data ownership, access, and privacy in a cultural context, and propose a data-focused extension to the traditional process of participatory software design. We believe that this new software engineering process will contribute to the goal of data sovereignty for data obtained through IoT technology.

The appeal of solutions built on wearable and lightweight hardware is that they can contribute to the gathering of "big data" in a minimally-intrusive fashion. They can also be easily adopted by end-users in wearable solutions that provide increasingly-complex analytics about a variety of personal data metrics. This is seen in the continuing evolution of personal trackers measuring activities (walking, running, swimming, climbing etc.) and corresponding personal metrics (heart-rate, heart-rate variability, galvanic skin response).

These wearable solutions typically provide a variety of visualisations to support end-users in understanding and using this data to improve their performance or measure themselves against others. Wearable technologies have also been adopted in several ways in work environments, using sensors that track GPS location and provide lightweight communications, body position alarms etc. They are increasingly being seen as ways to protect workers in challenging environments such as firefighting (Parker et al., 2017), policing (Baber et al., 2005), and the armed services (Scataglini et al., 2015). A large focus of the research in the areas of IoT and wearable technology is, understandably, based around security and privacy,

as evidenced by 7,820 publications mentioning wearable, IoT, security and privacy out of 14,200 publications on wearable IoT listed by Google Scholar since 2018 alone. Ensuring data cannot be intercepted or *stolen* by malicious entities is essential in all networked solutions. The challenges are increased in IoT solutions where a wide variety of different types of hardware are joining and leaving the network in ad-hoc ways and are reliant on a variety of cloud solutions for analysis and storage of streaming data. Ensuring users have control over how their data are used, and by whom is also gaining traction, particularly in light of legislative controls such as the EU General Data protection Regulation (European Union, 2016).

Our focus in this paper is different, as we consider issues of data privacy and ownership from a personal and cultural perspective. That is, we request that the design of systems that will collect personal data from users must sufficiently respect concepts of data ownership as dictated by principles and guidelines for data sovereignty. These should be addressed at the design stages along with all other requirements. We aim to ensure that the people who are given access and ownership of the data collected are the *correct* people (we expand on this later) and that we respect the owners by ensuring they have full control of their data irrespective of how the designers of technical solutions that collect data are allowed to use it within their technical solutions.

The role that the cultural background of end-users plays in the design of technology solutions is well understood with respect to issues such as internationalisation, localisation, use of terminology, icons and symbols etc. However, the effect this has on data and data collection, particularly for indigenous and first-nation communities is not so well understood or addressed in the domain of software development.

In user-centred design, software designers often make the assumption that because they understand that the systems' users are different from them (the designers and technology providers) they can make use of appropriate methods to compensate for this and this will lead to technical solutions that are appropriate for diverse end-users. This has been understood since early days of computer science and human factors research, and a variety of approaches, tools and methods exist to support this. For example cultural probes (Gaver et al., 1999) and ethnographic study techniques (Fetterman, 1989) etc., which are intended to ensure software engineers understand and acknowledge these differences, have been around since the early nineties, and these form the foundations of ongoing and current research in this area. We further acknowledge that supporting end-users in both mono-cultural and cross-cultural environments requires us (as software designers) to understand and address both our own preconceptions and the reality and belief systems of these cultures. This information can then be used to support interface development and appropriate visualisations, e.g., as described by Yeo (Yeo, 1996).

Here, however, we consider something more fundamental, which is the cultural implications of collecting and using personal data within technological solutions such as IoT systems. Rather than only concerning ourselves with how to appropriately create solutions which use this data, we take a step back and first consider the appropriateness of collecting the data in the first place, and what this means in terms of cultural appropriation and data ownership. Both these concepts are considered in particular in the post-colonial context of Aotearoa New Zealand[1], in which cross-cultural design is further burdened by a persistent power imbalance between the cultures involved.

The research questions addressed in this article are therefore the following:

(i) What is a software engineering design process that considers data ownership as defined by the user's cultural norms?

(ii) To what extent can such a process be guided by appropriate tools or frameworks?

In this paper we address the issue of indigenous data sovereignty as it pertains to the collection of personal data within IoT solutions. We begin by describing the details of a particular use-case in New Zealand forestry, which we use as an example to discuss the issues and principles relating to data collection, data sovereignty and data ownership more generally. Although using this example puts the focus on data collection as it pertains to Māori (the indigenous population of Aotearoa New Zealand) we will discuss the wider implications of our work later in the paper. We then describe the concept of indigenous data sovereignty, with particular focus on the Aotearoa New Zealand context. The central ideas of this paper are then introduced as a new understanding of data management. We present a discussion on what this means for the design of IoT systems specifically and systems which gather personal data in general. We finish with concluding remarks and an outline of the next steps for this research.

3. HAKITURI PROJECT AND NZ FORESTRY

The proliferation of wearable technology, sensors and IoT solutions, alongside concerns about data privacy and use,

[1] We use the term Aotearoa New Zealand to refer to the country as a whole, while the country's forestry industry is customarily referred to as New Zealand forestry

means that the work we describe here is applicable across a wide range of use cases. However, for descriptive purposes in this paper we will focus on a specific example, which is drawn from our current research project, Tini o te Hakituri. This project focuses on the use of wearable and lightweight technology to support workers in hazardous work environments, specifically in New Zealand forestry.

The New Zealand forestry industry has an unacceptably high level of accidents and fatalities, with 40 recorded fatalities between 2011 and 2018, and 121 notifiable incidents reported to Worksafe NZ in the 12 months prior to December 2018 (Worksafe New Zealand, 2019). An independent review was conducted in 2014 to try to identify potential contributors to this poor safety record. This identified, amongst others, that lack of training, worker fatigue and poor health and safety processes were all important factors (Adams et al., 2014). The review was based on a series of interviews with various interested parties (forestry management companies, contractors, workers etc.), but lacked any independent data from the workplaces. Our starting point when we began working with forestry was, therefore, the idea of collecting data from workers using wearable technology and sensors to understand more about their working environment and workloads (Bowen et al., 2015). Our initial studies in this domain gave us some insights which changed the way we considered tackling the problem and also uncovered information which forms the background to this work.

In our earlier research we used wearable technology to monitor aspects of worker activities (physical workload, steps taken etc.) and personal physiological measures (heart rate)(Griffiths et al., 2017). It became clear that considering this data without understanding its wider context was problematic. For example, if we take a simple measure such as heart rate and we perceive that a worker's heart rate has become elevated for an extended period of time then we also need to know what the worker is doing during that time. If they are engaged in physical activity such as felling trees in hilly terrain, then the elevated heart rate is to be expected and is of no concern. However, if the worker is a machine operator and has been sitting in the cab of his vehicle for a long period of time then the elevated heart rate is more concerning as it suggests that something other than physical activity is the cause. Contextual data encompasses a wide range of measures which might be personal (worker's role, current activity, or underlying health/fitness) or environmental (temperature, humidity, nature of the terrain being worked in, etc.) This led to plans to develop a solution that goes beyond personal measurement and to early designs for an IoT system consisting of both personal and environmental sensors (Bowen et al., 2017).

One aspect that we found during early explorations was that worker buy-in was difficult to obtain as any tracking of workers is understood as a *management tool* (Bowen et al., 2015). This is not surprising as it reflects observations from the literature: workers will reject solutions that seem invasive even if there is a clear safety benefit as they do not trust that the data will be used solely for that purpose. In our example domain one way of supporting safety is to identify workers who are potentially at risk because they are fatigued. However, if workers are monitored to identify if they are fatigued then there is a reasonable fear that this could lead to them being sent home as unfit for work (and therefore not being paid or ultimately losing their job).

Another important consideration in our research was the understanding that the workforce has a high number of Māori workers compared with other industries. According to an industry census 38.5% of forestry workers identify as Māori, which is 27.2% higher than the total Aotearoa New Zealand workforce (Competence, 2012). As we began to look at ways of gathering, storing and using personal data, it was necessary to take this into consideration both in terms of the nature of the data we might collect, and how it was stored, used and attributed.

The Hakituri project aims to shift the approach to one where the data is not taken and used autonomously, but rather is gathered and used in different ways to enable workers and their communities to support themselves and each other. As part of this we need to fully understand the consequences of collecting personal data (and using and storing it) when a large part of the workforce are Māori. That is, we must incorporate the necessary cultural concerns and appropriate data management systems to support these. This aims to ensure that the workers who we collect data from feel appropriately treated and respected. Our belief is that this may lead to more engagement and support from both the workers and their communities, because the benefits will be tangible and data collection mechanisms ethical and suitable for their needs.

We include the Hakituri project here to describe our initial motivations and also in order to provide illustrative examples for our discussions later in the paper. It is not intended as a case-study description and this is not a paper about the Hakituri project per se. For these reasons we do not give full details of the Hakituri design and implementation process.

4. DATA MANAGEMENT AND SOFTWARE DESIGN PROCESSES

We first outline standard software design processes and consider how data is typically addressed within these (Sommerville, 2010). Data is primarily considered as an artefact of the software: the focus is typically on how the

data is captured (input), how it is used and transformed (processed), and how results are reported (output). Figure 1 shows a simplified data flow of an IoT project that uses sensors to measure environmental data of a river. From the sensors in the river (data input), continuous data is sent to a unit that processes the incoming data stream, and matches the data to hazard patterns (analysis). This data may be stored for future analysis (storage symbolised by the database barrel). An environmental agency would be notified in case of emergency (data output). Similarly

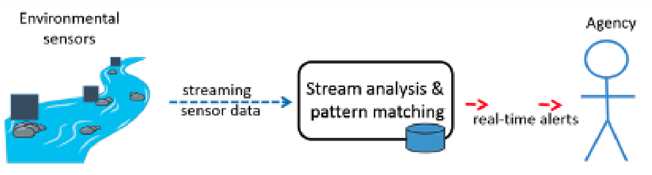

Figure 1. Dataflow example of environmental monitoring

in traditional monitoring systems (see Figure 2), the data flows from the wearable sensors that are attached to a firefighter. These streams are analysed by the system and presented to a person who monitors the incoming data streams from the crew and additionally receives alerts in case of emergencies. Any monitoring persons are considered to have the role of a data user, as they are consuming the data. Personal monitoring solutions, such

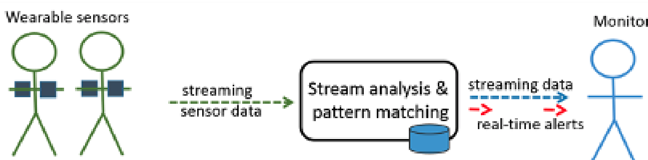

Figure 2. Dataflow example of worker monitoring

as activity trackers and smart watches, work in much the same way as Figure 2, however, they often involve hidden data users. In Figure 3, we show the data flow in which a person with a smart watch streams their data to a simple analysis software and receives real-time alerts (such as milestones in the steps walked). The person with the smartwatch sees themselves as the user of the watch and the data that is being collected. However, they typically cannot access their raw data but only simplified graphs. The aggregated and integrated data from all users is, however, collected and analysed at the service provider's side, who, overall, acts as the data user.

In all three examples there is little consideration of what the data is, where it comes from (beyond user

Figure 3. Dataflow example of personal smart watches and step counters

inputs) or any sense of ownership. Only when software engineers consider human factors relating to a proposed system are any personal attributes of the data considered, typically with focus on technical data management (e.g., ease of use, or how effectively information is provided back). They may consider how secure the system is to ensure the data is safe and kept private. But all of this is in the context of the data being a part of the system, which may include de-personalising and anonymizing of data. However, blanket anonymization is not always appropriate in a data sovereignty approach, as it removes the rights of data owners to access their individual data and understand its attributes.

The terminology that is typically used in software design also contributes to masking concepts of data ownership. Software engineers typically refer to 'users' as being the end-users of the software (Sommerville, 2010), but this does not make it explicit that they may also be contributors of data. To illustrate our new terms, and to clarify the way data sovereignty may influence software design, we now describe the dataflow for the Hakituri project, see Figure 4. We combine aspects of data flow from the examples given in Figures 1 to 3, together with an overall change in data ownership and management consideration.

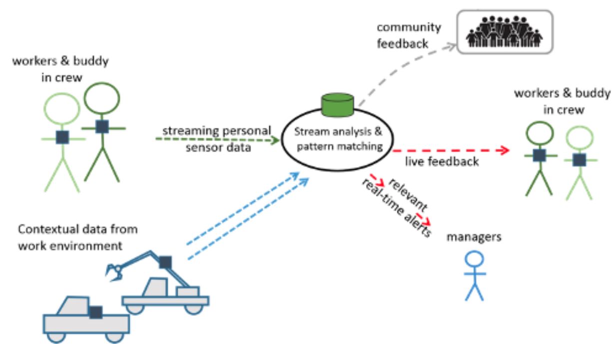

Figure 4. Dataflow in Hakituri

The workers in a crew wear smart shirts with sensors that measure indicators of fatigue, see top-left in Figure

4. This personal data will be streamed to the system together with environmental and contextual data from the work environment (lower-left). The data is analysed for fatigue and hazard patterns – the resulting information will be made available to the worker crew, and also the worker's community (whānau). The manager is informed about relevant information only, such as accident alerts. Note that the workers appear as both contributors and consumers of the data. Similarly, the company provides data about their machinery, as well as consumes data via the manager. Each of the contributors will keep ownership of their aspects of the data. As a consequence of this changed setup in comparison to Figures 1, 2 and 3, we also need to clarify terminology within the software engineering process to acknowledge the new roles that the various actors have in comparison to the traditional model. We will use the following terms for the roles:

- Data-contributing users: these are users of the system that is being developed who will provide data to the software (e.g., workers and their buddy within a crew)
- Data-consuming users: these are users of the system who will consume data (e.g., whānau and communities, manager, workers and their buddy within the crew)
- Data-contributing stakeholders: these are stakeholders with an interest in the system (such as forest management companies) who provide business data to it (e.g., machine owner and business owner)

Not shown in the figures above are the software engineers who develop the system and who have access to the data, but not ownership or any vested interest in the data beyond its function within the system. For systems involving human users, we expect that software engineers would follow best-practice, which would typically include the use of *Participatory Design* methods. The term "Participatory Design" encompasses many different practices (for example collaborative prototyping, focus groups, design workshops and design games etc.), it intersects with user-centred design practice (Norman and Draper, 1986) and may also include co-design, but central to all of these is the understanding that the users of a system are central to the design process and all stakeholders must play a role within that process (Simonsen and Robertson, 2012). Participatory design approaches recognise that the introduction of technology to work, or everyday life activities will transform those activities. Conflicts are likely to arise from this and will become part of the design processes, where they should be resolved by the active participation of all stakeholders (Bødker et al., 1995).

Figure 5 is a simplified overview of the participatory design process in software engineering which reflects the inclusion of stakeholders during various requirements gathering and design iterations.

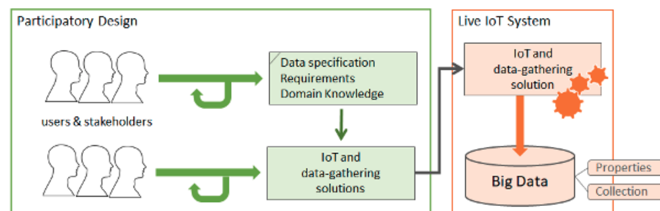

Figure 5. Participatory Design in software engineering an IoT system

Participatory design methods are iterative processes in which users and stakeholders are actively involved in the software design process. Users and stakeholders bring domain knowledge to the design process, which informs the data specifications and system requirements. These in turn are then used by the software engineers to create a software solution, which is tested and critiqued by users and stakeholders. Through a number of iterations the final software solution is arrived at. An IoT system may gather streams of data that over time create big data collections, which ideally follow the technical properties defined through the software design process. We now attempt to decouple the data from the technical solution and consider how within technical solutions in general, and IoT solutions in particular, the nature of the data means that software engineers should not separate the data from the contributing users.

5. INDIGENOUS DATA SOVEREIGNTY

The concepts of Indigenous data sovereignty. (Kukutai and Taylor, 2016b), and indigenous intellectual property (Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities, 1993), are about the data rights and interests of indigenous peoples. It is the right of Indigenous peoples to determine the means of collection, ownership, access, use, and dissemination of data pertaining to the Indigenous peoples from whom it has been derived, or to whom it relates (Snipp, 2016). In the Aotearoa New Zealand context, the Matātua Declaration on the Cultural and Intellectual Rights of Indigenous People (Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities, 1993) recognises Māori ownership of their cultural and intellectual property and the importance of ensuring that indigenous descendants are the primary beneficiaries of indigenous knowledge and this has been reinforced by Article 31 of the United Nations Declaration on the

Rights of Indigenous Peoples (UNDRIP) (United Nations, 2008) which directly addresses indigenous control over data and information. The principles of UNDRIP express the importance of geographical and cultural context as well as self-determination of communities through meaningful participation (Yap and Yu, 2016). The rights of indigenous people have been stated in the country's founding constitutional document, the Treaty of Waitangi of 1840 (Kukutai and Taylor, 2016a). The Māori version of the Treaty – Te Tiriti o Waitangi – promises in Article 2 to uphold the rangatiratanga (authority) of tribes over their land and tāonga (treasure) (tto, 1840). Māori data is thus subject to the rights stated in the Treaty of Waitangi and in the UNDRIP.

The Māori Data Sovereignty Network asserts that "Data is a living tāonga", and declares the guiding principles of rangatiratanga, kotahitanga (unity), manaakitanga (generosity) and kaitiakitanga (guardianship) (Te Mana Raraunga, [n.d.]). The charter recognises the need for attention at both governance and operational level. In particular, data may support the expression of Rangatiratanga (sovereignty/autonomy). The charter emphasises the potential contributions of ethical data-use and identifies as key consideration the need to identify appropriate data guardians and the principles by which they will operate.

Snipp (2016) defines the following requirements for data sovereignty in a post-colonial world: data governance has to ensure that

(i) Indigenous peoples have power to determine who should be counted among them (who belongs and who should be excluded for the purposes of data collection);

(ii) Collected data reflects the interests, values and priorities of Indigenous peoples (with focus on core values transcending narrow interests);

(iii) Tribal communities not only dictate the content of data collected about them, but also have the power to determine who has access to these data.

Our work in the Hakituri project is guided by these principles, and those of Te Mana Raraunga. It is our aim to ensure that affected Māori communities achieve indigenous data sovereignty over data that is acquired using ICT processes (and particularly IoT system use). We believe the traditional software engineering design processes have to be changed to incorporate participatory design processes that recognise indigenous data rights. In addition, as non-Māori we must also consider how Western research practices traditionally disadvantage and distance Māori from "real participation and voice" (Berryman, 2013). Revitalised traditional indigenous practices and ways of theorising, known as Kaupapa Māori, resists traditional Western research methodologies and seek to balance unequal power relations (Smith, 1991). While most Kaupapa Māori methodologies focus on collaboration and communication, none of these consider an ICT context.

Our hypothesis is that indigenous data sovereignty is equally important for IoT solutions which gather personal data from individuals within a particular cultural group. Furthermore, while for our project a person's streaming data within a small time window is of particular relevance, the history of the data of a community will easily grow into big data proportions. As we have described earlier, it is customary for data aggregation and anonymization strategies to be adopted in technical solutions, but this may lead to loss of whakapapa (genealogy) information about data-contributing users (e.g., person-specific health and relationship context) and thus act as a barrier to access to data at both the individual and collective level (cf. whakapapa information being one of the dimensions of Te Mana Raraunga Framework).

Existing indigenous data sovereignty approaches such as Te Mana Raraunga guidelines have been used for analysing access rights to existing large data collections, such as census records, and to record collections that are only slowly changing over time, such as health records (Statistics New Zealand, 2007). Here we are concerned with the new collection of rapidly growing data sets (time series). IoT connections are expected to grow beyond 20 Billion by 2020 (Gartner, 2017). Automatic analysis of IoT data requires compliance with laws of the countries in which data is collected (Weber, 2010). Data privacy concerns, such as over leaks of personal data from fitness apps and gadgets, are being addressed by new legislation, such as the European General Data Protection Regulation (GDPR) (Wachter, 2018). However, no clear methods exists yet as to where and how to store the IoT-originated data, and how and to whom give access to the data (Castelluccia et al., 2018).

6. A NEW UNDERSTANDING OF DATA MANAGEMENT

We previously considered different aspects and levels of sensitivity of (IoT) data based on its value to different individuals and groups who provide, use and manage it (Bowen et al., 2017; Hinze et al., 2018). Here we argue that all personal data belongs to the individual generating it and its aggregation and collective use should be owned, governed and driven by those individuals as well as their communities. The idea of personal data belonging to those from whom it is collected is not new, the increase in use of data as a *currency* where it is traded for

some technical solution (such as activity trackers which gather a user's personal activity data and then presents them with aggregated information drawn from this) has similarly seen an increase in concerns about how this is implemented in practice. Often it is far more beneficial to those collecting the data and the real owners of the data are not getting the true value of this in return (Gates and Matthews, 2014).

We further argue that it is not just ownership that is relevant, but also the locations of storage and types of use that must be considered, particularly with respect to cultural identity and data sovereignty. While our focus is on Māori workers and their communities, Whānau (family) and Iwi (tribes), we believe this to be equally true for all people and the communities they identify with (for example a collective of workers in a factory, or a small rural community working collectively in agriculture). In the Hakituri project, data from forestry workers belongs individually to the worker and collectively to their communities, who are then charged with using the information to keep their communities safe. Our role as technology developers and providers is to present the data in ways that are meaningful to them and allows them to achieve this.

Ownership of data means the right to use it in ways that the owners see fit (which may not match our ideas or initial requirements) and which are not governed or controlled by the technology provider. A large dataset of forestry worker activities and inferences drawn from this data could be seen as having a high commercial value to forest owners and forestry management companies, but its use in this way may not reflect the wishes of the owners of the data, i.e. the workers themselves. Sometimes, of course, there may be a blurring of boundaries between individuals and communities, such as iwi or whānau-owned forestry management companies.

We propose that as part of initial requirement gathering, we likewise perform a cultural analysis of the data that may be collected within the end product, and engage with the data-contributing users to ensure we develop solutions that gather and use the data in culturally sensitive ways. To do this we need some mechanism for understanding the data within different cultural frameworks. Of course, in our context in Aotearoa (and likely other indigenous populations) no such framework exists for collecting data in the way we propose. We explore the Te Mana Raraunga framework for large data collections and consider how this may fare in our context of use.

The data gathered within the Hakituri system can be categorised across various dimensions, e.g., personal, contextual, business-related. Here we focus on ensuring data sovereignty, and so we consider the different elements of the data within that context.

7. STARTING POINT: TE MANA O TE RARAUNGA FRAMEWORK

We propose the following initial steps when dealing with IDS in conjunction with IoT solutions:

(i) Identify relevant frameworks, tools or processes for considering data with the relevant communities (a) where necessary specialise these for the specific context (b) where nothing exists for a particular community this will need to be developed from existing artefacts (for example based on a more general set of principles such as the GDPR (European Union 2016).

(ii) Analyse the data that will be collected, processed and stored by and within the IoT system, using the methods identified in (i)

(iii) Develop a data plan which describes the results from (ii)

(iv) Develop the data agreement for the users based on (iii)

For our forestry example, we use resources provided by Te Mana Raraunga in step (1) above, however this is not as straightforward as merely utilising existing tools or following structured guidelines. For step (1a) therefore, we needed to specialise the Te Mana Rauraunga principles and practices to work within an IoT development process. Te Mana Raraunga provides a framework that defines data use and data users across relative dimensions (Hudson et al., 2017). Figure 6 outlines how, for example, data use is governed by the value and originality of the data, how it is to be used and the level of trust associated with this use. The data users are then considered by their relationship to the data as well as their expertise and authority, which should guide their level of responsibility. The central spirals represent (black) Tapu, which is to be sacred or prohibited and its counterpoint, (red) Noa, meaning unrestricted. Figure 6 is a high-level representation of the principles and guides the reader to consider the balance (what we may refer to as 'trade offs') between different properties. For example, when we think about how data is used we must balance the value of the data (Tika) with the level of trust required for users of that data (Pono). The higher the value the higher the level of trust that is required. The aim of the framework is to assess data use and users along these dimensions in order to identify aspects that are tapu or noa. To practically incorporate these considerations the framework is supported by assessment questions (see Figure 7) that help determine these properties. The table in Figure 7 lists the concepts from the framework, along with their characteristics and a question that should be

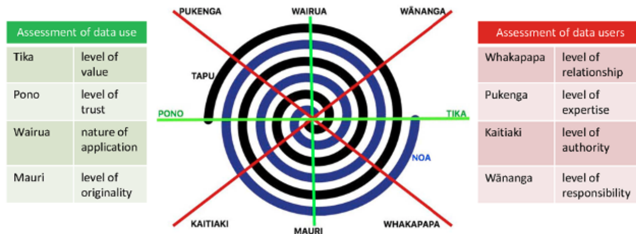

Figure 6. Te Mana o te Raraunga Framework, centre, (Hudson et al., 2017) with author annotations

Concept	Characteristic	Assessment Question	high	med	low
Tapu	Level of sensitivity	How sensitive is the data?			
Noa	Level of accessibility	How accessible should this data be?			
Tika	Level of value	How does the use of this data add value to the community?			
Pono	Level of trust	Will the community support this use of the data			
Mauri	Level of originality	How unique is the data			
Wairua	Nature of the application	Is the data being used in the same spirit as its original purpose?			
Whakapapa	Level of relationship	Does the user have an existing relationship with the data?			
Pukenga	Level of expertise	Does the user have the expertise and experience to use data in a culturally appropriate manner?			
Kaitiaki	Level of authority	Will the data be protected from inappropriate use?			
Wananga	Level of responsibility	Does the institution have the necessary infrastructure to ensure the use of the data in a culturally appropriate and ethical manner?			

Figure 7. Assessment Questions from the Framework (Hudson et al., 2017) with coding reference (Hudson, 2018)

asked to determine the level of impact this has for the given data. The colour-coded columns to the right of the table are used to indicate these levels (High, Medium or Low) on a scale, with red indicating 'most'.

The first step for the Hakituri project (1) was identifying the Te Mana Raraunga resources and then (1a) analysing the terminology in the context of IoT development. For example, where the assessment questions relate to *data* there is an expectation that there is a single dataset, whereas in IoT we deal with multiple streams of data from different sources, new data being generated by the processing algorithms, and finally a big dataset (which is the combination of all of these). We cannot, therefore, treat all parts of the data in the same way. For each of the relevant terms, we therefore mapped out what the matching concepts were in the development process. Some examples are given in the following (partial) list:

- Data - all of the personal and contextual data collected, inferred and reported by the system
- Access - real-time direct to worker via alerts, apps, software
- Access - real-time direct to buddies via alerts
- Access - post hoc to supervisors via aggregated reports
- Use of Data - alerting to workers, buddies, supervisors
- Use of Data - personal filtered information to whānau

Initially we expanded the assessment questions to deal with each identified data component individually, we then moved on to do the same for 'data users'. We broke the data and users down into atomic components and then used these, so that instead of one row for the data collectively, we instead had multiple rows. Figure 8 shows some examples of the outputs from this. However,

Concept	Characteristic	Assessment Questions	Atomic Data Component	High	Med	Low
Tapu	Level of Sensitivity	How sensitive is the data?	Worker personal biometric			
			Worker role			
			Worker inferred fatigue level			
			Worker location			
			Contextual location			
			Contextual temperature			

Figure 8. Expanded Assessment Questions

it soon became clear that this would prove intractable as we began to expand on each of our defined sub-categories for data, user, use etc. We required a more holistic approach to the data and system consideration which aligned better with the users and stakeholders. This took the form of discussions and hui (meetings) where alongside traditional participatory design activities (typically intended to elicit functional and non-functional requirements) we addressed the wider concerns relating to the data ecosystem. The initial data analysis steps (1 and 1a) informed step 2, where we used our general understanding of the principles to investigate the data and users. Steps 3 and 4 were then accomplished both prior to, and during, the participatory design activities. For the Hakituri project we also included all of the data gathered and analysed within that participatory design, which led to a separate data plan agreement for that data. Details of how this was implemented can be found in (Rolleston et al., 2021).

The framework and assessment questions from Te Mana Raraunga, therefore, acted as a starting point for these discussions rather than presenting a complete solution.

8. EXTENDING THE PARTICIPATORY DESIGN FRAMEWORK

We propose that the methods used to identify relevant properties and considerations of data for different cultural groups in the manner shown in the previous section is integrated with traditional participatory design processes. In Figure 9 we show how the two parts are intended to run in parallel, with existing design activities in the bottom part of the figure and what we call 'Participatory Data Design' activities in the top part of the figure. Again, we do not specify particular participatory design activities

here, rather we group all, or any, such activities under the umbrella term. Our belief is that in all circumstances we should enhance these activities to support the inclusion of data and data ownership considerations. Obviously the

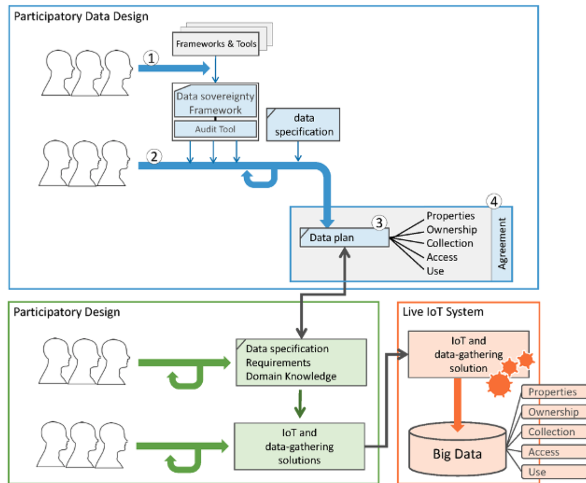

Figure 9. Extended participatory design framework

framework as used in our example is not appropriate for all contexts. Preparing a suitable way of evaluating the data for the cultural context therefore becomes the first step in the design process, i.e. the first part of the "Participatory Data Design" in Figure 9. In the general case then, the steps required to follow the process are those proposed in the previous section:

- **Step 1:** Identify appropriate frameworks for considering data with the relevant communities (if these do not exist then they must be prepared in consultation with the relevant communities);
- **Step 2:** Audit the proposed data using the mechanisms identified in Step 1 with all of the user groups and stakeholders;
- **Step 3:** Develop a data plan that specifies the results of Step 2;
- **Step 4:** Develop a data agreement for the users that encompasses the outcomes of Steps 2 and 3

For the Hakituri project this led to the following outcomes:

- **Step 1a:** Identification of the Te Mana Raraunga framework, assessment questionnaire and data audit tool as appropriate for the context of the project
- **Step 1b:** Specialisation of these resources for an IoT development process (as described in 7)
- **Step 2** Analysis and categorisation of different types of data and users, leading to discussions with the research team and Māori partners within participatory design hui
- **Step 3** A data plan describing how data for the project would be managed, and how the participatory design data would be returned to the participants.
- **Step 4** A high-level plan to be incorporated into the software development and implementation process which will become part of the end-user acceptance criteria.

In addition, working through each of these steps requires appropriate leadership, which for the Hakituri project meant our Māori research partners. As part of the requirements gathering process we ran a series of hui (meetings) and participatory design workshops with Māori forestry teams. Once we had created an initial plan for how we wanted these to work we handed over ownership of the process to our Māori research partners who took leadership in running these. There were of course challenges in making this work, particularly for the non-Māori researchers who had to step back and acknowledge the expertise of our Māori partners. One of the outcomes of this was that the information gathered during participatory design was considerably richer than we would usually expect, and was viewed through a Te Ao Māori (Māori worldview) lens first and foremost. It also meant we had an obligation to also include the data gathered during the participatory design process under the same data plan, and therefore we were required to return that data to the groups that provided it. A more detailed discussion of these parts of the process is given in (Rolleston et al., 2021).

The full data plan outlines the results of the steps above and allows us to dictate how the data will be gathered and used within the technical solution. The data agreement encompasses wider concerns such as how and where the data is stored (including physical storage on particular servers), how long it is kept for, who will have access in the future etc. The issue of physical storage is particularly pertinent for indigenous data sovereignty as one of the key principles is that storage of the data be governed by the laws of the land of the people it is collected from. This means that most standard cloud services are not appropriate (certainly in Aotearoa New Zealand) as the servers are not physically in the country which has ownership of the data. Note, while there are some Aotearoa New Zealand servers for cloud storage (for example via catalystcloud.nz and www.omninet.co.nz), there are no guarantees that the data will never leave the country. In addition, storage on Aotearoa New Zealand servers does not guarantee access

and management according to the principles of indigenous data sovereignty. Finally, NZ-based storage solutions are potentially more expensive than those from larger overseas providers, and may therefore not be the preferred solution for every stakeholder.

9. DISCUSSION

We here outline how the contributions of this article relate to, and are situated within, the topics of decolonisation in HCI, participatory design, and questions of data ownership. While concepts of cultural ethics in ICT development have been widely discussed in other fields Capurro (2008); Carbo and Smith (2008), by contrast our approach is focussed on technological details and software development processes.

9.1. Culture and indigenous communities

The discourse of decolonisation is developing within HCI and Design fields, however, established models and practices are seldom questioned (Smith et al., 2021). The notion of *post-colonial computing* acknowledges that all computing and design research / practice is culturally located, and affected by power imbalances (Irani et al., 2010). A number of HCI researchers have acknowledged this situation, but very few have explored the impact on the ways data management and data guardianship are designed in computing projects. Research on cultural aspects of participatory design focus typically on suitable methods to elicit system functionality (e.g., Winschiers-Theophilus et al. (2015); Plimmer et al. (2015a)) or explore interface and interaction design (e.g., Santoso and Schrepp (2019); Smith-Jackson et al. (2019)). Authors such as Winschiers-Theophilus and Bidwell Winschiers-Theophilus and Bidwell (2013) go further in their questioning of Western HCI paradigms, and propose an Afro-centric guide to interaction design. Wider understandings of post-colonialism and its impacts on research continue to evolve and we position our work here as part of that discourse. For example, Duncker's work undertaken twenty years ago, considered cross-cultural usability implications for Māori (Duncker, 2002) from the perspective of a non-Māori researcher. In Aotearoa New Zealand, and probably other parts of the world it is no longer acceptable to view indigenous communities as 'other' in this way (or 'the Māori' as Duncker refers to them), rather the expectation is that such research involves and/or is led by indigenous researchers. It is one of the reasons this paper focusses on the technical practice rather than the specific example of the Hakituri project. The Hakituri participatory research work now sits with the Māori research team members rather than the computer science researchers. While authors such as Abdelnour-Nocera, Clemmenson etc. have focussed on identifying different practices and ways of working in HCI for different countries and cultures ((Abdelnour-Nocera et al., 2012, 2013; Sturm et al., 2015) are just a few examples) we suggest that we can build on such work and continue to improve by ensuring indigenous data-design practices are included and are community led.

In most cases, questions of data management and storage are typically referred to technicians and database administrators. Holeman et al. (2017) acknowledged the importance of negotiating values in a participatory process. We argue that questions of data management and guardianship are central values, and thus need to be addressed as part of a participatory design process which acknowledges rights and responsibilities to data of indigenous communities.

9.2. Research environment

While research methods that are participatory and decolonising have been discussed in a number of fields (e.g., health (Cochran et al., 2008; Simonds and Christopher, 2013) and geography (Herlihy, 2003)), these typically do not yet have far-reaching implications for data ownership and sovereignty. Questions of intellectual property rights were discussed in particularly for geographical mapping of indigenous places (Chapin and Threlkeld, 2001), but may be dismissed as "politicising" the research (Herlihy, 2003). Similarly, ICT projects involving interaction design with indigenous people (Plimmer et al., 2015b) rarely reported questions of data ownership, as they typically used small data sets, with no streaming data. Our proposed Participatory Data Design extends the well-known procedures of participatory design, e.g., (Schuler and Namioka, 1993). We also must acknowledge the different power balances that exist both in research and technical development. Kovach (2015) questions an "indigenising" of the western research model, which may use indigenous people as tokens. She acknowledges the debates in participatory design about how to be authentically participatory, but also emphasises the well-documented data politics of researchers "extracting" and publishing data with little benefit to the involved communities.

We focussed on specific properties of data and presented ways of incorporating cultural considerations into the management of such data. There are, of course, other important aspects that must be acknowledged when we conduct this type of research and develop technical solutions in this way. Within our research team, for example, there are implications for the non-indigenous members of the research team. Expertise in Human Computer Interaction and data streaming in technical

solutions has to take a back seat to cultural knowledge in some cases. In the case of the Hakituri project, this meant hiring experts on Māori participatory research practices to lead the discussions with Māori worker groups. The non-Māori research team provided the context for the participatory design hui, but the Māori research practitioners then took the lead on this part of the design process both in running the hui and in analysing the resulting data. We cannot assume that as non-Māori our software engineering processes take precedence, if we genuinely want to engage in participatory design then we must acknowledge that the leadership of the design hui belongs to the domain expert (the Māori researchers) and not with the software engineers.

We must also learn new ways of conducting research and engaging with methodologies in ways that may be different to our usual approaches but which are respectful and appropriate for the cultural context.

9.3. Data ownership

While we target personal data as being most susceptible to being gathered and used in ways likely to disrupt appropriate cultural sensitivities we must also be careful to include other data that likewise has cultural implications. For example Māori have relationships with the land they live on, and the water and air that sustain them. Data which captures properties from these sources may likewise be considered *personal* as it pertains to iwi and the communities that have relationships to these. This is likely to be true for other indigenous populations and requires that we understand what these relationships are.

As our data come from multiple sources (data-contributing users as well as data-contributing stakeholders), "personal ownership" is not a simple concept as it pertains to different parts of the data. In the case of technical solutions in a hazardous work environment such as those for the Hakituri project, there is also a factor of worker activities being part of their job role (for example, workers in machinery which provides context data from the work environment). There is, therefore, a further blurring of the boundaries of ownership. For example if we track a user's location throughout the day, that may have commercial sensitivity and meaning beyond that of the individual (if it can be used to infer information about workplace terrain or location of resources). Ownership may need to be shared, which may also mean that certain users and stakeholders have different views of parts of the data (aggregation and anonymization) depending on the outcome of these discussions.

9.4. Long-term data management

One aspect omitted in this paper so far is a discussion of storage of data, which forms an important part of indigenous data sovereignty. Data needs to be governed by the laws of the land it is collected in, which in most cases rules out cloud storage. We do not currently have a long-term storage solution in the Hakituri project but recognise its importance for future work. Furthermore, although our focus is on indigenous data ownership we acknowledge relationships to considerations raised by, for example the GDPR (European Union, 2016). The right to data portability and to increased control over personal data, therefore, requires potential rethinking of data handling in all future ICT projects and for all users. The work that we have presented here offers a methodology to address this.

10. CONCLUSIONS

In this paper we discussed cultural data considerations within IoT and described a process for incorporating this practically into participatory design within the context of the Hakituri project, which collects data from Māori workers in New Zealand forestry.

After exploring Te Mana o te Raraunga framework for applicability to streaming data in the Hakituri project, we proposed "Participatory Data Design" as an extension to the classic participatory engineering design process, incorporating the use of frameworks and tools that specifically focus on indigenous data sovereignty.

We note that the goal of indigenous data sovereignty will not be automatically achieved through the suggested software engineering design process. It relies on the software engineers to fully engage in the process, not only as a token activity. If good practice is not followed, the resulting software may be unethical, ignorant of data ownership, or otherwise flawed.

We discussed the wider implications of this approach for participatory research in ICT. While we acknowledge that our research domain is particular and its specifics will rarely apply to other projects, we believe that our experience as described in this paper outlines a way forward for researchers who have similar concerns in other circumstances. Many application domains have to manage data that is highly personal and sensitive, with or without cultural aspects, and the methodology outlined is suitable to be adopted more widely and can contribute to data management considerations more generally.

Acknowledgements

We wish to acknowledge Anna Rolleston and Erina Korohina from Te Manawa Ora.

REFERENCES

1840.
Te Tiriti o Waitangi.
Te Reo version at http://www.treaty2u.govt.nz/the-treaty-up-close/treaty-of-waitangi.

José L. Abdelnour-Nocera, Torkil Clemmensen, and Masaaki Kurosu. 2013.
Reframing HCI Through Local and Indigenous Perspectives.
Int. J. Hum. Comput. Interact. 29, 4 (2013), 201–204.

José L. Abdelnour-Nocera, Mario Michaelides, Ann Austin, and Sunila Modi. 2012.
An intercultural study of HCI education experience and representation. In *Proceedings of the 4th International Conference on Intercultural Collaboration, ICIC '12, Bengaluru, India, March 21-23, 2012*, Ravi Vatrapu, Vanessa Evers, K. B. Akhilesh, Bonnie A. Nardi, and Martha L. Maznevski (Eds.). ACM, 157–160.

G. Adams, H. Armstrong, and M. Cosman. 2014.
Independent Forestry Safety Review – An agenda for change in the forestry industry.

Chris Baber, Paul Smith, James Cross, Damien Zasikowsk, and John Hunter. 2005.
Wearable Technology for Crime Scene Investigation. In *Ninth IEEE International Symposium on Wearable Computers (ISWC 2005), 18-21 October 2005, Osaka, Japan.* 138–143.

Mere Berryman. 2013.
Kaupapa Māori: The research experiences of a research-whanau-of-interest.
Culturally responsive methodologies (2013), 263–286.

Elisa Bertino. 2017.
Security and Privacy in the IoT. In *Information Security and Cryptology - 13th International Conference, Inscrypt 2017, Xi'an, China, November 3-5, 2017, Revised Selected Papers.* 3–10.

Susanne Bødker, Kaj Grønbæk, and Morten Kyng. 1995.
Cooperative design: techniques and experiences from the Scandinavian scene.
Human-Computer Interaction (1995), 215–224.

Judy Bowen, Annika Hinze, Sally Jo Cunningham, and Richard Parker. 2015.
Evaluating Low-cost Activity Trackers for Use in Large-scale Data Gathering of Forestry Workers. In *Proceedings of the Annual Meeting of the Australian SIGCHI OzCHI'2015.* 474–482.

Judy Bowen, Annika Hinze, Christopher Griffiths, Vimal Kumar, and David Bainbridge. 2017.
Personal Data Collection in the Workplace: Ethical and Technical Challenges. In *Proceedings of the 31st British Computer Society Human Computer Interaction Conference* (Sunderland, UK) *(HCI '17)*. BCS Learning & Development Ltd., Swindon, UK, Article 57, 11 pages.

Rafael Capurro. 2008.
Intercultural information ethics: foundations and applications.
Journal of Information, Communication and Ethics in Society (2008).

Toni Carbo and Martha M Smith. 2008.
Global information ethics: Intercultural perspectives on past and future research.
, 1111–1123 pages.

Claude Castelluccia, Mathieu Cunche, Daniel Le Métayer, and Victor Morel. 2018.
Enhancing transparency and consent in the IoT. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 116–119.

Mac Chapin and Bill Threlkeld. 2001.
Indigenous landscapes.
A Study in Ethnocartography. Arlington: Center for the Support of Native Lands (2001).

Patricia AL Cochran, Catherine A Marshall, Carmen Garcia-Downing, Elizabeth Kendall, Doris Cook, Laurie McCubbin, and Reva Mariah S Gover. 2008.
Indigenous ways of knowing: Implications for participatory research and community.
American Journal of Public Health 98, 1 (2008), 22–27.

Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities. 1993.
Mataatua Declaration on cultural and intellectual property rights of indigenous peoples.
First International Conference on the Cultural & Intellectual Property Rights of Indigenous Peoples, Whakatane, Aotearoa, New Zealand.

Competence. 2012.
Forestry Cluster Needs Analysis.
online at http://troq.competenz.org.nz/assets/TROQ/Documents/Forestry/Needs-Analysis-Report-Forestry-22112012-final.pdf..

Elke Duncker. 2002.
Cross-Cultural Usability of the Library Metaphor. In *Proceedings of the 2nd ACM/IEEE-CS Joint Conference on Digital Libraries* (Portland, Oregon, USA) *(JCDL '02)*. Association for Computing Machinery, New York, NY, USA, 223–230.

European Union. 2016.
Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Official Journal of the European Union L 119, 1 (2016).

D. M. Fetterman. 1989.
Ethnography: Step by step.
In *Applied social research methods series.* Vol. 17. US: Sage Publications, Inc.

Gartner. 2017.
Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent from 2016.
Gartner Press Release 27 February 2017.

Carrie Gates and Peter Matthews. 2014.
Data Is the New Currency. In *Proceedings of the 2014 New*

Security Paradigms Workshop (Victoria, British Columbia, Canada) *(NSPW '14)*. ACM, New York, NY, USA, 105–116.

William W. Gaver, Anthony Dunne, and Elena Pacenti. 1999. Design: Cultural probes. *Interactions* 6, 1 (1999), 21–29.

Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. 2019. Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things* 5 (2019), 41 – 70.

Christopher Griffiths, Judy Bowen, and Annika Hinze. 2017. Investigating Wearable Technology for Fatigue Identification in the Workplace. In *Human-Computer Interaction - INTERACT 2017 - 16th IFIP TC 13 International Conference, Mumbai, India, September 25-29, 2017, Proceedings, Part II*. 370–380.

Peter H Herlihy. 2003. Participatory research mapping of indigenous lands in Darien, Panama. *Human Organization* (2003), 315–331.

Annika Hinze, Claire Timpany, Judy Bowen, Carole Chang, Nicola Starkey, and Hinemoa Elder. 2018. Collecting Sensitive Personal Data in a Multi-Cultural Environment. In *32nd BCS Human Computer Interaction Conference (BCS HCI 2018)*.

Isaac Holeman, Edwin Blake, Melissa Densmore, Maletsabisa Molapo, Fiona Ssozi, Elizabeth Goodman, Indrani Medhi Thies, and Susan Wyche. 2017. Co-design across borders special interest group. In *Proceedings of the 2017 CHI conference extended abstracts on human factors in computing systems*. 1318–1321.

Maui Hudson. 2018. Māori Data Sovereignty: Māori rights and interests in data. Keynote at Science Coding Conference, 2/8/2018.

Maui Hudson, T. Anderson, T. K. Dewes, P. Temara, H. Whaanga, and T. Roa. 2017. *He Matapihi ki te Mana Raraunga - Conceptualising Big Data through a Māori lens.* University of Waikato, New Zealand, 64–73.

Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E Grinter. 2010. Postcolonial computing: a lens on design and development. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1311–1320.

Margaret Kovach. 2015. *Emerging from the margins: Indigenous methodologies.* Canadian Scholars' Press, 19–36.

Tahu Kukutai and John Taylor. 2016a. *Data Sovereignty for Indigenous People: Current Practice and Future Needs.* Australian National University Press, 1–24.

Tahu Kukutai and John Taylor (Eds.). 2016b. *Indigenous data sovereignty: Toward an agenda*. Vol. 38. Anu Press.

Donald A. Norman and Stephen W. Draper. 1986. *User centered system design: new perspectives on human-computer interaction.* Lawrence Erlbaum Associates, Hillsdale.

Richard Parker, Antonios Vitalis, Robyn Walker, David Riley, and H. Grant Pearce. 2017. Measuring wildland fire fighter performance with wearable technology. *Applied Ergonomics* 59 (2017), 34 – 44.

Beryl Plimmer, Liang He, Tariq Zaman, Kasun Karunanayaka, Alvin W Yeo, Garen Jengan, Rachel Blagojevic, and Ellen Yi-Luen Do. 2015a. New interaction tools for preserving an old language. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 3493–3502.

Beryl Plimmer, Liang He, Tariq Zaman, Kasun Karunanayaka, Alvin W. Yeo, Garen Jengan, Rachel Blagojevic, and Ellen Yi-Luen Do. 2015b. New Interaction Tools for Preserving an Old Language. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. ACM, New York, NY, USA, 3493–3502.

Anna Rolleston, Judy Bowen, Annika Hinze, Erina Korohina, and Rangi Matamua. 2021. Collaboration In Research: Weaving Kaupapa Māori And Computer Science. *AlterNative: An International Journal of Indigenous Peoples* 17, 4 (2021), 469–479.

Harry B Santoso and Martin Schrepp. 2019. The impact of culture and product on the subjective importance of user experience aspects. *Heliyon* 5, 9 (2019), e02434.

S Sarkar. 2016. Internet of Things—robustness and reliability. In *Internet of Things*, Rajkumar Buyya and Amir Vahid Dastjerdi (Eds.). Morgan Kaufman, 201–218. https://doi.org/10.1016/B978-0-12-805395-9.00011-3

Sofia Scataglini, Giuseppe Andreoni, and Johan Gallant. 2015. A Review of Smart Clothing in Military. In *Proceedings of the 2015 Workshop on Wearable Systems and Applications* (Florence, Italy). ACM, 53–54.

Douglas Schuler and Aki Namioka. 1993. *Participatory design: Principles and practices.* CRC Press.

Vanessa W Simonds and Suzanne Christopher. 2013. Adapting Western research methods to indigenous ways of knowing. *American Journal of Public Health* 103, 12 (2013), 2185–2192.

J. Simonsen and T. Robertson. 2012. *Routledge International Handbook of Participatory Design.* Taylor & Francis.

Graham Hingangaroa Smith. 1991. *Reform and Māori educational crisis: A grand illusion.* Research Unit for Māori Education, University of Auckland

Auckland.

Rachel Charlotte Smith, Heike Winschiers-Theophilus, Daria Loi, Rogério Abreu de Paula, Asnath Paula Kambunga, Marly Muudeni Samuel, and Tariq Zaman. 2021.
Decolonizing Design Practices: Towards Pluriversality. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–5.

Tonya L Smith-Jackson, Marc L Resnick, and Kayenda T Johnson. 2019.
Cultural Ergonomics: Theory, methods, and applications.
CRC Press.

C Matthew Snipp. 2016.
What does data sovereignty imply: what does it look like?
Australian National University Press, 39–76.

Ian Sommerville. 2010.
Software Engineering.
Addison-Wesley, Harlow, England.

Statistics New Zealand. 2007.
Snapshots of New Zealand: integrated data infrastructure.
`https://www.stats.govt.nz/integrated-data/integrated-data-infrastructure/`.

Christian Sturm, Alice Oh, Sebastian Linxen, José L. Abdelnour-Nocera, Susan M. Dray, and Katharina Reinecke. 2015.
How WEIRD is HCI?: Extending HCI Principles to other Countries and Cultures. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, Seoul, CHI 2015 Extended Abstracts, Republic of Korea, April 18 - 23, 2015*, Bo Begole, Jinwoo Kim, Kori Inkpen, and Woontack Woo (Eds.). ACM, 2425–2428.

Te Mana Raraunga. [n.d.].
Te Mana Raraunga: Māori Data Sovereignty Network Charter.
online at `https://www.temanararaunga.maori.nz/s/Te-Mana-Raraunga-Charter-Final-Approved.pdf`.

United Nations. 2008.
United Nations declaration on the rights of indigenous peoples.
`https://www.un.org/esa/socdev/unpfii/documents/DRIPS_en.pdf`.

Sandra Wachter. 2018.
Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR.
Computer law & security review 34, 3 (2018), 436–449.

Rolf H Weber. 2010.
Internet of Things–New security and privacy challenges.
Computer law & security review 26, 1 (2010), 23–30.

Heike Winschiers-Theophilus and Nicola J Bidwell. 2013.
Toward an Afro-Centric indigenous HCI paradigm.
International Journal of Human-Computer Interaction 29, 4 (2013), 243–255.

Heike Winschiers-Theophilus, Tariq Zaman, and Alvin Yeo. 2015.
Reducing" white elephant" ICT4D projects: a community-researcher engagement. In *Proceedings of the 7th International Conference on Communities and Technologies*. 99–107.

Worksafe New Zealand. 2019.
Notifiable incidents: Report on serious and immediate risk of harm.
online at `https://worksafe.govt.nz/data-and-research/ws-data/incidents/`.

Mandy Yap and Eunice Yu. 2016.
Data sovereignty for the Yawuru in Western Australia.
Australian National University Press, 233–252.

Alvin Yeo. 1996.
Cultural User Interfaces. A Silver Lining in Cultural Diversity.
SIGCHI Bulletin 28, 3 (1996), 4–7.

Congyingzi Zhang and Robert Green. 2015.
Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network. In *Proceedings of the 18th Symposium on Communications & Networking* (Alexandria, Virginia) *(CNS '15)*. Society for Computer Simulation International, San Diego, CA, USA, 8–15.