Emerging Trust Implications of Data-Rich Systems

Bran Knowles
Lancaster University

ABSTRACT
Pervasive technologies are enabling an increasingly data-rich world that is mediated through a broad spectrum of often highly interdependent systems. The data science surrounding these systems is rapidly transforming nearly every aspect of our lives. But how trustworthy are the systems and data upon which we have come to rely? This paper explores the complex collaborations and interdependencies that mediate trust-formation, and examines six challenges in generating and sustaining trust in the context of data-rich systems.

Author Keywords
Trust, data-rich systems, pervasive computing.

INTRODUCTION

Pervasive technologies are enabling an increasingly data-rich world that is mediated through a broad spectrum of often highly interdependent systems, and the data science surrounding these systems is rapidly transforming nearly every aspect of our lives. As the Internet of Things (IoT) agenda advances, more and more "things" in our environments are fitted with sensors that feed systems used to inform critical decisions, as in cases such as disaster management, health, and policing (e.g. [13]). Embedded sensors in wearables and personal devices generate data that can be processed by users' apps to assist with routine decision making, motivate behavior change, and satisfy personal interest, while also in many cases being sold to third party organizations to target advertisements and perform big data analyses. Individuals also have an abundance of tools to enable intentional production of data (e.g. social networks, content management systems, file sharing) — data that is often then put to creative and potentially unanticipated use by others. Organizations, too, are producing more data. Having increasingly made the transition from paper based records to digital archives, organizations are adopting new systems to analyze this data to make sense of opportunities for greater efficiency, profitability, and respectability. This in turn has helped them to identify additional data requirements — such as those that would enable new collaborative capabilities between stakeholders [7] — spurring yet higher volumes of data production.

Numerous personal, organizational, and societal-level transformations have resulted from this explosion in data and in the development of new systems for processing that data. As data systems have become fundamental to contemporary life it is crucial that they be trustworthy, but do we know — or know how we would determine — whether we should trust these systems?

Although a familiar concept in computing literature, trust has meant different things in different contexts. Here trust is defined as *a subjective assessment of the reliability that a person or system will perform an expected action* [8]. In this paper, the trust implications of data-rich pervasive systems are explored, and in particular six challenges are identified in making these systems trustworthy. Note that this work considers *human perceptions of trust*, as compared with early initiatives on trust that focused on securing hardware and software infrastructure (see **Prior Work on Trust**). It also explores trustworthiness as a characteristic of whole systems, going beyond (and yet incorporating) considerations of data accuracy.

PRIOR WORK ON TRUST (SUGGESTED SIDEBAR)

Previous work on trust has identified three broad categories that comprise a holistic trust research agenda (see [8])[1]:

Trust in data. Accuracy is typically considered the key characteristic of trusted data. Relevant research explores issues pertaining to 1) mobile data collection in resource poor scenarios that require accurate data (e.g. [14]), 2) mobile data collection in remote work scenarios (e.g. [7]) where data collected in the field is often difficult to verify or recollect, or 3) crowdsourcing and participatory sensing (e.g. [5]), where individuals collecting data are unskilled in the data collection. A system that relies on inaccurate data unknowingly or without appropriate qualification of the results it may produce is undeserving of trust, but accuracy in itself is not sufficient for ensuring that users believe a system to be trustworthy. Users may doubt the accuracy of data if, for example, they are unable to verify it. Hence, trust in data results from the confluence of data accuracy and satisfactory communication of this accuracy.

Trust in systems. In the context of 'trusted computing', trust is understood as a technical property of systems. The Trusted Computing Platform Alliance (www.trustedcomputinggroup.org/), for example, focuses on the development of security standards as key to system trustworthiness. Similarly, trust is often discussed in relation to privacy [10]; i.e. users must have a degree of confidence that the system protects their identity and personal information. Relatively under-explored, in contrast, is the fact that systems sit within a larger system-of-systems, each reliant on and responsible to other systems. A system that produces trustworthy results for its intended context may not be sufficiently trustworthy when used to feed other algorithms, particularly those designed for contexts where the consequences of inaccuracies are more problematic.

Trust in people. Trust is also a characteristic of interpersonal relationships, and in collaborative computing contexts this relationship is mediated through systems that compensate for a lack of co-location or natural social ties (e.g. the structure of an organizational setting) by providing mechanisms for fostering interpersonal trust. For example, whereas in 'real world' situations trust develops over time as a person consistently demonstrates their reliability, reputation systems (e.g. [17]) provide quick access to information about a user's past behavior by aggregating others' user ratings. Related research also explores trust dynamics between stakeholders, and how systems can help foster greater trust through, for example, providing groups with greater insight into other stakeholders' activities and motivations [7, 5]. More work in this area is needed to understand how human perceptions of the trustworthiness of systems is entangled with inter-personal dynamics that enfold in the use of these systems.

CONTEXT

To motivate this paper, trust issues are considered in a typical pervasive scenario, namely that of wellbeing. This includes a broad range of technologies aimed at individuals who are seeking to lead healthier lives. Especially popular are tools designed to help users improve fitness levels, such as activity trackers, which combine data from various onboard sensors (e.g. accelerometers, barometers) to provide pedometry and actimetry information, often alongside biometric data (e.g. heart rate), GPS, and in some cases more advanced kinetic analyses (e.g. stride, foot landing) [15]. Often consumer fitness tools have a persuasive component, incorporating pervasive technologies to deliver context-aware information that is timely and relevant to the user's goals for changing behaviors (e.g. eating, exercise and smoking) [6].

The context of wellbeing is chosen here, in contrast to 'health', as an example domain where untrustworthy data would not be immediately catastrophic or life threatening. True health systems undergo stringent testing along numerous dimensions to ensure the accuracy of their

[1] These categories should not be understood as entirely distinct from one another. Trust in data, systems and people are all interconnected, and cannot be teased apart in practice. They are discussed separately here as a way of understanding constituent pieces of this trust puzzle, of which this paper's six challenges address various components.

output; whereas systems designed for non-expert use often trade off data accuracy for data availability. For lay consumers who are interested in improving their health and who otherwise lack insight into how to increase their fitness, it is argued that, "Data of lower precision but higher availability is better than high-precision but non-existing data" [15]. What has not been explored, however, in this context and others that make a similar trade-off, are the trust implications of these systems, which regardless of the precision they are able to deliver must nonetheless attend to users' perceptions of their trustworthiness. As will be shown, there are difficult challenges in designing trustworthy data systems — beyond technical advancements that improve the accuracy of sensor data — and important consequences of untrustworthiness that ought to be considered.

A hypothetical but imminently feasible pervasive system is presented, as follows, as a means of illustrating these challenges and consequences. The 'FangleBangle' is a wristband with mini display that recommends adjustments to the wearer's exercise routine. These recommendations are informed by actimetry and heart rate data along with environmental data including weather and air quality. Users set a goal for how many calories they would like to burn in a day, and the FangleBangle will help them reach this goal by anticipating a shortfall in necessary activity and suggesting the best times to exercise outdoors or suggesting time at the gym. Activity shortfalls are predicted based on the user's accumulated activity history and the fullness of the user's daily calendar. Exercise time and location recommendations are informed by aggregated weather data and sensor readings of pollution and pollen levels, while taking into account the immovable events in the user's calendar (e.g. meetings, picking up children).

CHALLENGES

Having described a typical pervasive system, this section explores six challenges in developing trustworthy data systems that apply to this system. Note that these challenges are not unique to the system described, and should pertain to a wide array of data systems. Nor are the challenges presented here intended as a comprehensive list. The aim is to offer insight into the research opportunities to be had in attending to trust in the domain of pervasive computing.

Getting at the 'ground truth'

One of the ways people might be able to determine the trustworthiness of new information, and new systems, would be to test against things they know. Google Maps is an example system where users would be able to perform this test fairly easily, i.e. by searching for their own house. People are uniquely qualified to verify the accuracy of a map of the area around their house if they have lived there for any length of time, having enough knowledge to assess:

- Is the high level information correct? —e.g. are the streets where they are expected to be?
- How detailed is this map? — e.g. does it also show known footpaths?
- How current is this map? — e.g. does it show recent additions to the house (e.g. a new orange roof)?

All of this information helps users determine how much they should trust Google Maps when they are going to (or looking at) an area that they are unfamiliar with.

Most data systems do not have such obvious potential for users to independently verify the trustworthiness of the data against things they know well. In cases where data systems produce entirely new information — as opposed to presenting old information in new ways — how will people prove to themselves that the data they present is accurate, sufficiently detailed, and up-to-date? Verification of sensor data is especially difficult in many cases. In the FangleBangle example, with pollen sensors, pollution sensors, and weather feeds all being taken from different sources, users would need to verify simultaneous readings in multiple places at once to demonstrate the trustworthiness of the data. Furthermore, much of the data used by FangleBangle cannot be easily observed and/or measured. Without professional equipment, verifying pollen and pollution levels is impractical. Similarly, a user would struggle to verify the

accuracy of the actimetry information. While it is possible to (at least roughly) verify pedometry information, if a user pays close attention to how much they are walking, it is more challenging to verify the other data used in calculating the number of calories burned. For example, while the user may have a general sense of their heart rate, measuring their heart rate accurately for comparison would require precise equipment. And lastly, sensors are often placed where individuals physically cannot go, or measure details that are too minute for people to measure with anything other than the sensor itself (e.g. the Sensoria smart sock: http://www.sensoriafitness.com/).

The first challenge in supporting trustworthy pervasive data systems is therefore *how to provide appropriate mechanisms to enable users to access personally verifiable information*. Although there are other ways people establish trust in the systems they use, there may be none so persuasive as having access to this 'ground truth', so it is important to explore what data users would need access to — and how it should be communicated — for them to be able to subjectively verify a system's trustworthiness.

Mapping the data flow

Much of the existing work on trust and data notes the importance of provenance [2]. It is clearly important to know where data has come from, as this helps in determining whether the source of the data can be trusted to be accurate, honest and unbiased. But what has largely been neglected is the importance of knowing where data is going *to* as part of assessing the trustworthiness of the system (or system of systems) as a whole.

In other arenas, such as food and consumer safety, there are historic examples of the vulnerability created when individuals in a long distribution chain are unaware of where their products are going. To attend to this problem, legislation was introduced forcing traders to record who they traded with on both ends (who they bought from and who they traded to) in order to enable systemic recalls when a certain component in that chain was faulty or contaminated [4, Article 18]. Thus far, no similar legislation exists for data systems, so data is being passed from system to system without any accounting of these increasingly complex distribution chains.

This presents a situation whereby a faulty sensor, rogue agent or simple error might be perpetuated throughout a very long chain of interdependent systems without detection. This is especially worrying in the case of intentional sabotage by pranksters or cyber-terrorists[2]. In the case of FangleBangle, it is conceivable that a faulty environmental sensor could lead to suggestions for users to exercise in dangerous conditions of poor air quality, potentially exacerbating hayfever and asthma and increasing exposure to carcinogens. Assuming FangleBangle (or another system making use of this same sensor data) is able to detect the error through independent air quality measurements, system administrators would be able to contact those maintaining the data feed they are using, who may or may not be the owners of the rogue sensor in question. Without knowing the precise source of data (i.e. which exact sensor and who owns it) used by the system, FangleBangle would have to pass any complaints down the distribution chain. This is not impossible, but it is inefficient. More problematically, however, if the owner of the rogue sensor detects malfunction, without knowing which systems are using this data, it is not possible to pass warnings and corrections up through the distribution chain to all relevant parties. Hence the second challenge is *how to support comprehensive mapping of data distribution chains*.

The problem here is not so much that we can't trust the data that is passed through multiple interdependent systems, but rather that we seem far too trusting of a digital infrastructure in which there is no traceability, and therefore no quality assurance, for the data we have become so reliant on. Perhaps legislation will be what ultimately forces us to map our data distribution chains in the way we do for food safety: each system must keep records of where they get all the data they use, and who they pass their data to — a step beyond devices simply 'calling home'.

---

[2] Note a major UK investment into research to address problems such as this: https://www.epsrc.ac.uk/funding/calls/compatriotsresearchhub/.

Understanding trust in the aggregate
It is increasingly rare these days for systems to rely on a single source of data. Aggregating data streams enables interesting, complex analyses, but it also makes determining a system's overall trustworthiness a far greater challenge. Data systems can bring together far more data sources than a person is capable of mentally juggling, and/or rely on data sources for which a user is ill-equipped to assess (or incapable of assessing) their trustworthiness.

The trustworthiness of a system is highly dependent upon the trustworthiness of the sources they use. For example, FangleBangle would make flawed recommendations if it relied on only one source for pollution data; but if pollution data were itself aggregated from numerous sources, one of them being inaccurate would be less problematic, as the error would be mitigated by the other data being accurate.

If, however, the wristband's pedometer over-counted significantly, the system would not recommend enough exercise for the user to meet their daily calorie burning goal; and if the activity history data were inaccurate, FangleBangle might anticipate a shortfall in necessary daily exercise and recommend activity when a user would already have met their goal (or vice versa). In both of these cases, even if the air quality data is accurate it is not enough to make the system trustworthy. The third challenge, therefore, is *how to enable users to gauge the trustworthiness of constituent data sources in determining a system's overall trustworthiness*.

As a pre-requisite in attending to this challenge, users would need at a minimum to be able to access a list of data sources used in the system's calculations. More helpful, however, might be the development of a formalized vetting process for data systems, e.g. a recommender system for data sources, so that users might gain insight into the trustworthiness of these listed sources without having to determine it for themselves.

Handling complexity
Whether a system can be trusted to correctly interpret data is integrally related to the design of the system algorithms themselves. In most cases, however, the user will not have the requisite knowledge to interrogate the algorithm at all, much less evaluate its trustworthiness.

Even at a conceptual level, these algorithms can be highly complex. Using the FangleBangle example, calculating a single calorie burned is an immensely difficult challenge related to kinetics and chemistry, i.e. how much movement, and what kind of movement, will burn a calorie? But even determining how much and what kind of movement a user engages in requires multiple algorithms that infer movements from accelerometer and barometers in the wristband. The fact that it is worn on the wrist introduces additional variables that need to be accounted for in the algorithm. While a user may be able to experiment with the device and determine that actimetry data is less accurate when the FangleBangle is worn on the wrist as opposed to being worn at the hip, without understanding how the algorithm determines movements they are unlikely to be able to make changes that would improve these readings. The fourth challenge, therefore, is *how to provide users necessary insight into the system's underlying algorithms without placing a significant or unreasonable expectation on users.*

There is an existing body of work that might be further developed in this area. For example, [3, 12] found that providing explanations as to why a system behaved a certain way led to greater user understanding and, consequently, trust. At the same time, improving the intelligibility of data systems is no trivial task, and indeed it has been argued that intelligibility negatively impacts user trust for context-aware systems that are relatively uncertain of their actions or results [11]. This suggests that new approaches to intelligibility may need to be explored especially for these low-certainty applications. And in addition to offering explicit explanations regarding the expected behavior of systems, it is worth exploring *feedforward* techniques [16] — i.e. interface design, visuals and subtle cues that help users understand what to expect — as a route to increased trust.

Deciphering motivations and biases
This challenge is concerned with the fact that data systems tend to provide (or indeed have) very

little information about the motivations of the people *creating* both the data itself and the algorithms that comprise the data system.

Motivation and bias is an especially under-examined topic in the context of pervasive technologies, as sensor data is often assumed to be inherently objective. Consider, however, the pollution sensors that feed into FangleBangle, which may be placed by organizations with definite political motivations for reflecting either high or low pollution levels. It is possible that pollution readings for a user's area are taken from the local council who, keen to demonstrate compliance with governmental ordinances to improve air quality, placed the majority of its sensors in parks and residential areas. Had the FangleBangle drawn from sensor data collected by an organization principally concerned with environmental issues and motivated to record data that reflects the scale of the problem as they perceive it, sensors might be placed in high traffic areas or situated lower down on lamp posts where pollutant levels are greater. Also relevant to how sensor data might be skewed is the motivation of the individual person doing the sensor placement. A person who is paid per sensor might be rushing, placing sensors wherever convenient; a person who feels passionately about air quality might be more careful in their placement. There are many motivational factors that influence the accuracy of the pollution data, none of which are known to, accounted for, or represented by the FangleBangle.

Given that knowing a person's motivation is deeply relevant to determining the trustworthiness of the data they create (cf. Theory of Reasoned Action [1]), it is essential that strategies are developed for accounting for these motivations. For example, revealing the identity of data contributors may enable users to infer their motivations, but this would need to be balanced against privacy and safety concerns. One possible solution might be to enable ratings of sensor data providers. But clearly, taking it on faith alone that people are well intentioned, unbiased and committed to the accuracy of the data they produce creates enormous potential for both inaccuracy and manipulation. Hence the fifth challenge is *how to provide appropriate information to enable users to decipher the motivations that may bias the data system's output*.

As the above example illustrates, this is as relevant to data creation as it is to algorithm creation, in that it would be misleading for a system making inferences based on pollution levels to draw solely from on-street sensors while discounting other available sensors that are placed in lower-emissions areas. The challenge here is not how to eradicate selectivity bias (which may be unavoidable); instead, it is how data systems might convey inherent biases to the end users. Understanding which data was included or excluded, why, and how this has shaped the system's output may help a user determine its trustworthiness, especially when compared to another system that uses different criteria based on more (or less) sound reasoning.

Moderating trust

One of the unfortunate characteristics of trust is how hard it is to gain while being extremely easy to lose [5, 8]. Regardless of a system's historical reliability, a single failure opens the door for people to re-examine their perceptions of its trustworthiness, potentially eradicating all hard-won trust if sufficient reasons are not found for renewing that trust. Data systems often do not provide users such assurances when their faith is shaken — e.g. providing satisfactory explanations of the cause of the failure and steps taken to remedy it — as footholds to prevent trust slipping away entirely.

With FangleBangle, there might be several very good reasons why it may fail to produce sound exercise recommendations. One might be that the user has not worn it long enough for it to accrue sufficient activity history data to reliably predict how many calories they are likely to burn in the course of their day. Simply informing users of this issue (and providing an estimate of when it might have the data to perform more accurate calculations) could prevent the loss of trust. Another reason might be that the user's calendar is not sufficiently detailed or not up-to-date, and as a result the system frequently suggests exercise during times the user is busy. In this case, making it clear to the user how exercise times are decided by the system may encourage the user to do better at maintaining their calendar, or at the very least the user will know that they are to blame for the system's failure and are therefore capable of fixing it.

It is important to note that trustworthiness does not require perfection. If trust is understood as

a subjective assessment of the reliability that a person (or system) will perform an expected action (see **Introduction**), then part of being trustworthy is meeting expectations, but the other part is ensuring that the other party's expectations are reasonable. An example of the latter would be calling to inform a person if one is running late — admittedly less good than being on time in the first place, but it can prevent the kind of upset that leads to complete breakdowns in trust. With systems like FangleBangle, which make various inferences along the way to making a behavior change recommendation, a certain proportion of recommendations will inevitably be imperfect. Indeed, almost all analyses involve a margin of error — a detail which data systems are especially poor at conveying. If users expect FangleBangle to ensure they meet their exact calorie burning target every day, they will lose trust fairly quickly when expectations are not met. If on the other hand the system is honest about how frequently it is likely to help users meet their calorie burning goal within 5% of this target, the user is able to form more realistic expectations that the system will be better able to live up to, hence preserving the trust relationship.

The sixth and final challenge, then, is *how data systems might provide indicators that would enable users to appropriately moderate their trust in ways that prevent catastrophic losses of faith in their systems*. Bearing in mind [12]'s finding that providing information about why a system does not do something is not the most effective means of garnering user trust, the design solution here is nontrivial (cf. [9]). Designing for feedforward [16], however, may again prove useful here, preempting unreasonable expectations by providing information about what to expect from a system.

DISCUSSION

The challenges identified above clearly illustrate that supporting trustworthy pervasive data systems will require an interdisciplinary, multi-level approach that attends to both a) making systems *deserving* of user trust and b) fostering user *perceptions* of the trustworthiness of systems (cf. [7]). The first two challenges demonstrate that, in contrast to prior work that stresses the importance of data accuracy, trustworthy data is that which is not simply accurate but is *verifiably accurate* (challenge one); and the distribution of data must be handled in ways that enable quality assurance regarding the accuracy of data (challenge two). The next challenges demonstrate that, in contrast to concerns about the trustworthiness of technical properties of systems (e.g. security, privacy), systems-level trust results in addition from the ways in which systems combine (challenge three) and interpret data (challenge four), i.e. the resulting output must be reliably 'correct'. And the final two challenges demonstrate the influence of interpersonal trust dynamics in the perception of the trustworthiness of systems, specifically how trust assessments require an understanding of the motivations of data contributors (challenge five), and preventing catastrophic losses of trust involves attenuation of unrealistic user expectations (challenge six).

Moreover, the examples provided for the hypothetical wellness system, FangleBangle, illustrate that for the system to be deserving of user trust, several improvements are needed in areas external to the system itself—e.g. in the surrounding data eco-system or the legislative framework within which it operates. For example, ensuring that the data it relies on is accurate requires either a process for certifying sensor accuracy or a means of testing (e.g. spot checking) sensors, as well as a structure in place whereby other systems can alert FangleBangle of any faulty data. While in part FangleBangle can increase perceptions of trustworthiness by focusing on developing its user interface to better communicate the steps it has taken to make itself deserving of trust, the fact that systems such as FangleBangle are dependent upon other systems means that users' perceptions of trustworthiness must extend to the larger system-of-systems in which such systems sit. **Table 1** provides examples of potential implications for the need to support trust in systems such as FangleBangle. Reflecting the broad interdisciplinary nature of the challenges these are structured into three main areas: 1) the design implications related to effective communication of system's trustworthiness (i.e. *user interface* concerns), 2) the *technical* implications of ensuring that systems and the system-of-systems are deserving of trust (e.g. metadata and markup requirements), and 3) the *legal and policy* implications of increasing individual system trustworthiness given the high degree of interdependence between systems.

It speaks to the broader significance of this work that the implications presented in Table 1 are not especially specific to the hypothetical pervasive system described in this paper[3]. Consider, for example, a typical smart city system designed to help users locate available parking spaces. In order to be *deserving* of trust, this system must have up-to-date knowledge of the location of all potential parking spaces in a given area. The system, therefore, aggregates various data sets — some maintained by the local council, some by private companies — the motivations and perceived trustworthiness of which may be very different from one another. The system must also have accurate information about the availability of these spaces, which it draws from sensors placed in parking bays. Independently verifying the accuracy of the sensors that detect available spaces is impractical both for users and for system developers. If, however, the accuracy of these sensors were certified or otherwise externally verified, trust might more reasonably be placed in the data they produce. And yet, once in a while a car will damage a sensor, in which case it is important that the owners of these sensors (the car parks) know how to pass information about faults up the distribution chain to those relying on the data. In order to foster *perceptions* of the trustworthiness of the system, various steps might be taken. Firstly, the system could enable users high level insight into how the system identified spaces to foster confidence in the system's ability to make good recommendations. Secondly, to assuage concerns about potential hidden agendas (e.g. people generating data in ways to attempt to discourage parking in certain areas or increase revenue at specific car parking facilities), the system could help users access relevant information regarding the motivations of those responsible for the production of data coming into the system. And lastly, if there are sensors on only 95% of parking bays, it is possible that users could find an available space that was not recommended by the system, potentially eroding trust. The chances of such disappointment could be lessened if the system also provides an estimate of its confidence in recommending the closest available parking space.

There are concrete examples of similar systems starting to emerge (e.g. Barcelona's Parkimeter, which allows people to find as well as book parking spaces: https://parkimeter.com/).
While there is impressive uptake of such systems, does uptake indicate that people really trust these systems? In the case of smart parking, the consequences of relying on untrustworthy data are minimal, and ostensibly acceptable (e.g. you find a slightly less optimal parking space); but what happens if these systems are used to inform more critical decision making (e.g. city planning decisions including the building of more car parks)? Robust trustworthiness might not be necessary for every individual system *per se* were it not for the fact that the data from such systems often get incorporated into other systems. The growth of smart cities is but one example of a trend toward increasing reliance on and inter-dependence between data-rich systems, and a system that is "trustworthy enough" in one context may not be trustworthy when used for purposes not intended or anticipated.

It is easy to overlook the importance of trust in developing systems like the hypothetical FangleBangle or various smart city apps, but these are the sorts of systems that comprise the bedrock of a pervasive, increasingly unavoidable network of systems, and it is important to ensure that we are not building on quicksand. Going forward, developing systems that are truly deserving of trust is a multi-level, collaborative, and difficult challenge that will involve attending to the different challenge areas outlined above and addressing the technical implications, design implications, and legal and policy implications they raise.

CONCLUDING REMARKS

This paper has argued that developing trustworthy systems not only goes beyond technical properties of the systems (i.e. security), it is also integrally related to both trust in data and trust in people. Indicative of this dynamic, a system that relies on inaccurate data or is powered by flawed algorithms is inherently untrustworthy; and yet a system that produces reliably accurate

[3] While this list is not necessarily suitable to all pervasive data systems — and indeed there may be further domain-specific implications to explore in future work — it is proposed here that variations on these implications will still apply when substituting 'FangleBangle' and 'wellbeing' for many systems designed for other contexts.

output may not be trusted if users do not have access to evidence of the system's trustworthiness. In other words, in addition to ensuring that data is accurate and the system 'works', trustworthy systems are those that actively cultivate trusting relationships with their users.

Note that, clearly, not all pervasive data systems are untrustworthy. Indeed, where example systems can be found that appear to solve any of the problems identified here, these solutions should be deconstructed to help with understanding how success might be replicated in other systems. And yet, the six challenges identified in this paper reveal a state of affairs pertaining to a significant portion of data systems where people cannot understand the data or the processes that resulted in that data; they have no means of testing it; they have no information about the qualifications of the people creating the data (or data systems), or their assumptions, biases and motivations that influence that data production and interpretation; and they have no understanding of how various data systems interrelate and how to stop the perpetuation of bad data throughout the distribution chain. In terms of trust, this means that people have limited means of gauging or appropriately moderating their trust in data systems, and that systems have no means of protecting themselves against catastrophic losses of trust. Crucially, if there is no way of determining the trustworthiness of data systems, users cannot — or at the very least, *should* not — trust them.

This has important implications for pervasive computing. If people conclude that some data systems are untrustworthy but do not know which ones, they are much less inclined to use devices that generate data or feed data to them. Reduced uptake would in turn reduce the opportunities for researchers and developers to capitalize on the data that pervasive technologies generate in the exploration of new knowledge and new digital innovations. Lack of trust would also negatively impact deployment opportunities for future pervasive systems. It is essential, therefore, that consideration is given to the trust implications of data rich pervasive systems explored in this work so that we may foster greater trust in the technologies that mediate our emerging data driven society.

ACKNOWLEDGMENTS
This work has been inspired by research conducted as part of the FAITH: Building Trust Between Citizens, Local Authorities and Contractors project funded by the EPSRC/ TSB under grant TS/I002537/1. In particular, the author would like to thank Nigel Davies for his contributions to this discussion.

AUTHOR BIOGRAPHY
Bran Knowles has a PhD in Digital Innovation from Lancaster University, where she has worked as a Research Associate and Design Ethnographer on projects including FAITH: Building Trust Between Citizens, Local Authorities and Contractors. Contact her at bran@highwire-dtc.com.

AUTHOR EMAIL
bran@highwire-dtc.com

REFERENCES

1. Ajzen, I., and Fishbein, M. Belief, attitude, intention and behavior: An introduction to theory and research, 1975.

2. Buneman, P., and Tan, W.-C. Provenance in databases. In *Proc. SIGMOD'07*, ACM (2007), 1171–1173.

3. Cramer, H., Evers, V., Ramlal, S., Van Someren, M., Rutledge, L., Stash, N., Aroyo, L., and Wielinga, B. The effects of transparency on trust in and acceptance of a content-based art recommender. *User Modeling and User-Adapted Interaction 18, 5* (2008), 455–496.

4. Food Standards Agency. Guidance Notes for Food Business Operators on Food Safety, Traceability, Product Withdrawal and Recall. http://www.food.gov.uk/sites/default/files/multimedia/pdfs/fsa1782002guidance.pdf, July 2007.
5. Harding, M., Knowles, B., Davies, N., and Rouncefield, M. HCI, civic engagement & trust. In *Proc. CHI '15*, ACM (2015), 2833–2842.
6. IJsselsteijn, W., de Kort, Y., Midden, C., Eggen, B., and van den Hoven, E. Persuasive technology for human well-being: setting the scene. In *Persuasive technology*. Springer, 2006, 1–5.
7. Knowles, B., Harding, M., Blair, L., Davies, N., Hannon, J., Rouncefield, M., and Walden, J. Trustworthy by design. In *Proc. CSCW '14*, ACM (2014), 1060–1071.
8. Knowles, B., Rouncefield, M., Harding, M., Davies, N., Blair, L., Hannon, J., Walden, J., and Wang, D. Models and patterns of trust. In *Proc. CSCW '15*, ACM (2015), 328–338.
9. Kulesza, T., Stumpf, S., Burnett, M., Yang, S., Kwan, I., and Wong, W.-K. Too much, too little, or just right? Ways explanations impact end users' mental models. In *IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, IEEE (2013), 3–10.
10. Lauer, T. W., and Deng, X. Building online trust through privacy practices. *International Journal of Information Security 6,* 5 (2007), 323–331.
11. Lim, B. Y., and Dey, A. K. Investigating intelligibility for uncertain context-aware applications. In *Proc. UbiComp '11*, ACM (2011), 415–424.
12. Lim, B. Y., Dey, A. K., and Avrahami, D. Why and why not explanations improve the intelligibility of context-aware intelligent systems. In *Proc. CHI '09*, ACM (2009), 2119–2128.
13. Lorincz, K., Malan, D., Fulford-Jones, T., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M., and Moulton, S. Sensor networks for emergency response: challenges and opportunities. *IEEE Pervasive Computing, 3,* 4 (Oct 2004), 16–23.
14. Medhi, I., Jain, M., Tewari, A., Bhavsar, M., Matheke-Fischer, M., and Cutrell, E. Combating rural child malnutrition through inexpensive mobile phones. In *Proc. NordiCHI'12*, ACM (2012), 635–644.
15. Meyer, J., and Boll, S. Digital health devices for everyone! *IEEE Pervasive Computing, 13,* 2 (Apr 2014), 10–13.
16. Vermeulen, J., Luyten, K., van den Hoven, E., and Coninx, K. Crossing the bridge over Norman's gulf of execution: Revealing feedforward's true identity. In *Proc. CHI '13*, ACM (2013), 1931–1940.
17. Yu, H., Shen, Z., Miao, C., and An, B. A reputation-aware decision-making approach for improving the efficiency of crowdsourcing systems. In Proc. AAMAS '13, International Foundation for Autonomous Agents and Multiagent Systems (2013), 1315–1316.

Table 1. Implications for developing a trustworthy data system for wellbeing

	Legal and policy	**User Interface**	**Technical**
1. Getting at the 'ground truth'	• Certification process for environmental sensor accuracy as pre-requisite for allowing these sensors to become a data feed • Mandating the availability of pinpoint location data for a certain proportion of environmental sensors for spot check verification by a data quality authority (see above) and/or lay public	• Providing comparative data for context (e.g. 'Your heart rate is currently measured approximately that of a person of your age, height and weight jogging leisurely') • Standardization/ heuristics for displaying data quality certification, i.e. so users know where to find information about the accuracy of the environmental sensors	• Preservation of metadata linking data to its originating sensor • Marking date of data creation and/or frequency of sensor readings/updates
2. Mapping the data flow	• Compulsory data distribution chain mapping in both directions — where the system's data comes from, and where it goes	• Ability for systems to push alerts about faulty data or updates of new data to those that develop and maintain affected systems • Enabling quick search of relevant parties affected by faulty data in a way that preserves privacy and intellectual property	• Backwards and forwards provenance
3. Understanding	• Requiring data systems	• Development of a	• Preservation of data

trust in the aggregate	to make data source list available to users (i.e. as in food ingredients labeling)	reputation/recommender system for data sources (cf. TripAdvisor)	source ratings histories
4. Handling complexity	• Protecting intellectual property of system developers who offer users high level information about their algorithms	• Experimentation with designs for communicating information in ways that help users understand the 'thought processes' underlying system algorithms • Providing overview of how similar systems differ in the way calculations are derived	• Within-system provenance; i.e. revealing how data passes through and is manipulated by the system to produce the final output
5. Deciphering motivations and biases	• Requiring acknowledgment of alternative data sources excluded from the calculations, perhaps including an explanation of reason for its exclusion	• Detailed mapping of environmental sensor locations that enables virtual observation of its placement (e.g. Google Streetview for sensors) • Representation of known affiliations and influences for organizations publishing sensor data • Providing overview of how similar systems differ in the data sources they draw from	• Keyword and location tagging for data sets/sources to enable comparison with alternatives
6. Moderating trust	• Creation of guidelines for estimating whole system accuracy (e.g. how often, and within what percentage, does the system produce the correct result?)	• Providing help and troubleshooting for improving accuracy of system output	• Enabling users to flag erroneous output; attaching that flag to the device or system history to help determine the reason for (and likely frequency of) the error