IoT in the wild: what negotiating public deployments can tell us about the state of the Internet of Things

D Hay,, B Buyuklieva*, J Daothong†, B Edmonds†, A Hudson-Smith*, R Milton*, J Wood†*

**University College London, United Kingdom, d.hay@ucl.ac.uk, †London Legacy Development Corporation, United Kingdom*

Keywords: Internet of Things, privacy, in-the-wild, serious games

Abstract

The promise of IoT technologies is such that they represent as big a social and economic change as the invention of the Internet itself. From the way people consume media in their homes to structural changes in global employment through improved automation, IoT has the potential to touch all aspects of peoples everyday lives at domestic, national, and international scales. The size of this change and the unpredictability of the potential social effects of these technologies is precisely what makes research into them urgent, yet at the same time it is this scale and unpredictability that makes this research challenging to conduct.

In the field of Human Computer Interaction, methodologies such as 'in-the-wild' research, in which the emergent properties of a technology are discovered through the design and deployment of a device or system outside of the laboratory and in collaboration with the people with whom it is envisioned to be used by, have emerged to deal with some of these issues. Yet beyond the findings garnered through direct user engagement, negotiating an in-the-wild study is itself a challenging proposition: the needs of researchers, technology hosts, and potential user groups must be balanced, and the potential affordances of a technology are limited by their acceptability with these stakeholders. With reference to 'Tales of the Park', a public-facing IoT deployment developed in partnership with Queen Elizabeth Olympic Park, this paper outlines some of the key points of negotiation that made the deployment possible, and contends that these indicate broader social anxieties about the future direction of the Internet of Things.

1 Introduction

There has been a move in recent years away from lab-based studies in Human Computer Interaction towards 'in-the-wild' deployments. This methodology seeks a richer model of what affordances a technology might offer by prototyping in the context in which that technology is envisioned to be used. In so doing, it not only aims to build a fuller picture of how people use technology and to gain insights that cannot be gleaned in a lab-based study, but to discover the emergent user needs that might become apparent as people appropriate it for their own use [1].

There is a wide range of literature about the results, opportunities, and difficulties that in-the-wild studies present [2, 3, 4, 5]. However, a repeated theme within this literature is the problems that researchers encounter in negotiating, developing, and deploying technology in this way. What unites papers of this sort is that they demonstrate not only that in-the-wild methodologies are useful for discovering the affordances of new technologies, but that there is valuable learning to be gleaned about the possible social effects of those technologies from the process of implementing them. That is, the contexts in which these studies take place not only impact upon the design of the technology, but the very difficulties entailed by those contexts constitute valuable learning about how that technology might be used and what behaviours it might facilitate.

This paper contributes to this discussion with specific reference to 'Tales of the Park', an in-the-wild study focused on privacy and security issues related to Internet of Things (IoT) technologies conducted by researchers at UCL in partnership with Queen Elizabeth Olympic Park. In common with the aforementioned studies, the negotiations between the research team and the Park led to changes and compromises in the original research design, from which the research team learned a great deal. Drawing on our own experiences as researchers and on in-depth interviews conducted with key partners at Queen Elizabeth Olympic Park, this paper describes some of these compromises. We argue that these compromises themselves point to the epistemological boundaries of what can be discovered through in-the-wild methods; moreover, we suggest, that these boundaries align with the limits of the social acceptability of IoT technology itself, and indicate the sort of anxieties and ethical concerns that surround its future development.

2 Privacy, security, and networked devices

Tales of the Park was a technology probe designed to explore peoples understanding of the security and privacy issues that surround the Internet of Things. This term is somewhat imprecise in that it covers a range of technologies which include, in the domestic sphere, smart devices such as Amazon Echo, Google Home, and internet-enabled devices such as the Nest smart thermostat, smart lighting, and so on; [6] but also cheap, low-power, networked sensors which have the potential to rad-

ically reconfigure the management of urban space under the general rubric of the smart city. What underlies these disparate technologies is the fact that increasingly cheap microprocessor designs, in combination with widespread wireless networking technologies, means that it is becoming easier and cheaper to add data gathering, processing, and networking capabilities to more and more devices. Indeed, many of these new devices - such as the internet-enabled kettles and toasters which are at the time of writing becoming available on the open market - not only have not previously had anything to do with networked digital technologies, but it is difficult to see why they should need to do so now.

Whilst these technologies are currently in their infancy, they are becoming more widespread, and, as numerous authors have pointed out, are likely to become near-ubiquitous in technologically advanced societies in the very near future [7, 8, 9]. The proliferation and sophistication of these technologies bring a host of complex security and privacy implications for users, which are currently becoming apparent both to device owners and their manufacturers. Prominent examples of the sort of issues encountered in a domestic setting include the accidental ordering of products through the Amazon Echo [10]; the discovery that Samsung 'smart' televisions were sharing speech recordings of users with third parties in ways which were poorly explained [11]; or the My Friend Cayla' doll whose Bluetooth connection was revealed to be unprotected, potentially allowing third parties to listen to whatever was picked up by the doll's microphone [12].

These high-profile controversies are arguably related to the 'creepiness' or 'leakiness' (as defined by Shklovski *et al.* in relation to smartphone apps) of the devices concerned [13]. That is, they behave in ways which are unexpected to the user, they collect and process more data than seems reasonable given their intended function, or are insecure. But even disregarding these more prominent examples of mishaps in the IoT sphere, it is rapidly becoming apparent that adding computational and networking capabilities to devices changes them (and therefore our relationships with them) in fundamental ways. With the addition of computing and networking capabilities, what we might term the apparent and latent affordances of a device become radically altered. A networked toaster, for example, is no longer just a device for toasting bread - the devices principal and most visible affordance for the user - but potentially gains a host of other abilities which are far less obvious, if not invisible, to the user. It could have the capacity to analyse a user's consumption habits, which in turn could be used as a proxy for when they are at home or when they have guests, for example; or it could detect the other networked devices they have in their house. This data could then be sent back to the device manufacturer so as to gain market insight in ways which might be unexpected given the manifest purpose of the device.

Similarly, in an urban context, concerns have been expressed about the way in which the data which networked sensors gather has the potential to 'alter our patterns of behavior [...] without our being aware that it is happening' [14]. At its most beneficial, this could take the form of crowd analytics, modelling and subsequent intervention to improve the efficiency and safety of movement through stations at rush hour, as has been trialled on Londons Tube network [15]. More controversial potential uses include pervasive tailored advertising and, at its most extreme, the use of these technologies by private or state actors to shape behaviours in ways which subvert democratic norms [14].

Whether for good or ill, as theorists such as Benjamin Bratton have argued, the future ubiquity of these technologies has implications which are so wide-ranging that they represent a fundamental change in the nature of power in the contemporary era. The wholesale collection and analysis of data enabled by ubiquitous networked technology is a new method by which various state and non-state entities can understand the world and act in it [16]. More than this, however, the promiscuous nature of data - its capacity to move across and through networks with little regard to local, national, or international geographic bounds - changes the nature of political power itself, and even the concept of the nation state as codified in international law [17].

It should be obvious therefore that understanding how people might relate to these technologies - how they interact with them, to what degree they are aware of the way in which data moves around networked systems, and to what extent they consider the wider social implications of ubiquitous data collection that they enable - is therefore a pressing area for research. However, it is also one which is fraught with ethical and practical difficulties, especially when considered in the context of in-the-wild research.

3 Queen Elizabeth Olympic Park

Given the multifaceted nature of the issues raised by IoT, it is far beyond the scope of a single research project to address all of them. Tales of the Park, therefore, focused on three aspects in this field of study: to explore how people might react to intentionally leaky devices; how they understand how data flows operate within device networks; and to explore the affordances that natural language interfaces offer for demonstrating this data flow. In conducting this study, the research team had the opportunity to work in partnership with Queen Elizabeth Olympic Park (QEOP), a large public space in East London built for the 2012 Olympic Games.

The Park is managed by the London Legacy Development Corporation (LLDC), a public-sector organisation whose remit is to maximise the economic and social benefits of the Olympics through the redevelopment of the Park site and the immediate surrounding area. As such, since the Games the QEOP has undergone extensive repurposing, and there are at the time of writing around 4000 homes, eight permanent public venues, and an extensive building programme underway which includes additional housing, office, and retail space, and a number of ventures from major cultural institutions [18]. As part of these redevelopments, UCL is currently working with

the LLDC to build a new campus on the Park site. As a major partner and future tenant of the LLDC, UCL has therefore been granted access to the Park to conduct research activities, with Tales of the Park being one of a series of projects and studies ongoing as part of this arrangement.

As with any large public body, the LLDC have responsibilities to their visitors, their tenants, to local and national governments, and to the communities within and beyond the immediate boundaries of the Olympic site. Not only do they have to act in an ethical and responsible fashion, they must be seen to be doing so, in that they have a responsibility to protect both their own reputation as a public body and that of the Olympic Games legacy. As Ben Edmonds, the I.T. and Programme Change Manager at LLDC and the research teams principal point of contact through the design and deployment process put it:

"It's [the LLDC's] responsibility to make sure that this technology [...] is firstly worthwhile, having some tangible benefit, but also that it's not going be at the detriment of our visitors or local residents, whether that be an annoyance - an app, an IoT device bombarding them with spam or alerts every five minutes, or reducing the quality of their experience of this area, but also if we felt that there was any risk to public safety or security then its our responsibility to put our foot down and say 'this isn't going to happen'."

Moreover, the LLDC, through initiatives such as monitoring signups to its free WiFi network, and, as has been proposed internally, through the tracking of devices through that WiFi network for the purposes of footfall analysis, is collecting data about Park visitors through technological means.

As such, any attempt to address and explore the issue of privacy and security around technology in this space inevitably carries with it a certain element of risk. Therefore, whilst the opportunity to conduct research in such a public and widely-visited space is unusual, and represents a privileged opportunity to address questions which would be difficult to explore in other settings, it also entails compromise in order to allow the research to occur in a fashion which would be acceptable to all stakeholders. The challenge in the design of this study was therefore to devise an intervention which would both address the research domain and be acceptable (and comprehensible) for the Park and its audiences.

4 Designing Tales of the Park

From the outset, the project was conceived as an in-the-wild study with devices being deployed throughout QEOP for visitors to encounter. We wanted to find out how people would react to an unfamiliar device placed in public: would they trust it? What would they share with it? And what sort of behaviours would they engage in around it? In addition, as the debate around IoT both in the home and in public space evolves, the research team were keen to take the opportunity to raise awareness of these technologies in both their positive and negative aspects.

One specific problem space initially identified by the research team was the possibility of 'rogue' devices. As outlined above, the very cheapness of computing power is leading to a rapid proliferation of networked devices, and it is conceivable that malicious actors could place devices in public designed to compromise user privacy or gather data about them for unethical purposes. Initial design discussions therefore centred around creating devices which would explore these possibilities. It was apparent to the researchers that it would be possible, for example, to prompt users to disclose passwords; to track users through the Park and to inform them of where and how this was being done; or to use personal information solicited through a device to guess a user's identity. These possibilities, well within the capacities of available technology, speak very directly to the concerns that many people have about data collection in the public and private spheres, but are, for reasons that should be obvious from the above discussion, unacceptable both from an ethical and practical perspective. Whilst the research team anticipated that these more provocative interventions would be unlikely to make it into the final deployment, the issue was brought sharply into focus through conversations with stakeholders at the LLDC. As Ben Edmonds expressed it:

"A big part of [the issue] is of course cyber security, and the reluctance for us to put technology which the general public are unsure as to what it does, what information it collects [...] unless we can be transparent and be very forward with these people that are engaging with it about what its going to collect"

The possibility of putting rogue devices in the Park was therefore rejected at a very early stage. Yet in addition to this consideration, it became apparent as we worked with the Park that any intervention would need to - at least in part - align with the Parks business needs. Whilst any technology development pursued by UCL in relation to this project was done at no financial cost to the Park, no matter how 'light' an intervention is, it still requires the allocation of resources on the part of the Park to support it. A case needs to be made to the various stakeholders within the Park to justify this use of resources. As Jennifer Daothong, Head of Strategy and Sustainability at the LLDC put it:

"If it is a very short-term research project, the amount of work that has to go into addressing planning issues or speaking with our operational team, or responding to complaints about a website being down, or responding to enquiries about why it's not working and all that sort of stuff remains the same regardless of whether or not it is there for two weeks or if it's going to be there for a year or more."

Ultimately, if an intervention will lead to what Edmonds has described as 'quantif[iable], tangible benefits from a marketing perspective [or] an operational perspective' then it's much easier to get assent from these stakeholders to allow an intervention to proceed. Moreover, this need to get by-in internally

Fig. 1: A Creature installed outside the Aquatics Centre

relates also to the necessity for the Park to communicate the benefits of a technology to their public audiences:

"What I've found is that you have to do up front is not only as an organisation or district authority prove internally that this is worthwhile doing, you have to say up front to the people engaging with it, were not just collecting information for the sake of it; theres going to be a return on it, some benefit for you as well. And the Tales of the Park is a good example of this; we wanted to say to the people, not only is this going to be a fun, interesting thing for you to engage with, but the information we collect from you and others [...] in return we hopefully are going to make this area of East London and your Park experience, were looking to find opportunities to improve that."

Edmonds here suggests that there is a need to explain to Park visitors what any technological intervention is for, and that engagement with it will be worthwhile, be that in terms of it being fun, or that it will generate insights which could lead to improvements to the Park which could enhance the visitor experience. As a consequence of these concerns, instead of pursuing the more provocative but unacceptable interventions initially discussed, the final design of Tales of the Park used a series of proxies to explore the issues that surround data sharing and privacy in this technology space.

The final deployment therefore took the form of fifteen 3d-printed 'Creatures' - two honey bees, three bats, three otters and seven garden gnomes - deployed in the Park (Figure 1). Each Creature was connected to a text-based conversational agent through the use of a low energy Bluetooth beacon broadcasting a URL accessible through Googles 'Physical Web' platform. These prompted visitors to interact with the creatures via a non-intrusive push-notification to their smartphone. In this way, visitors were engaged by the Creatures, which then invited them to submit their personal memories of the Park and the surrounding area. Through the use of a cookie, visitor interactions with the individual creatures were tracked, which allowed the conversational agents to 'remember' users and their interactions with the devices. As all of the conversational agents were connected through the framing Tales of the Park website, interacting with one device on the network meant that users were in fact sharing data with all of them, which was then revealed to visitors as they interacted with subsequent Creatures.

The design of Tales of the Park, therefore, was a function of the necessity to create something that was viable to be deployed in a public space, addressed some of the Park's business needs in terms of collecting data to improve visitor experience, but was also relevant enough to be a proxy for understanding the privacy issues which surround connected devices. In our case, we have two proxies: 'memories' as a proxy for sensitive data; and beacon-enabled 'Creatures' as a proxy for a network of IoT devices. Memories functioned in two ways in this context: firstly, they allowed us to engage visitors with questions related to the Park and its environs, from which it would in principle be possible to gain insight from which improvements to Park services might be made; secondly, they are 'safe', in that they were willingly volunteered by visitors who were likely to share only things they felt comfortable with, particularly as they were informed by the agents that anything they shared with them would be 'remembered' and might be shared with others. The Tales of the Park system can therefore be conceptualised as a digitally-mediated agent network through which memories are shared between human and non-human actors, and which at the same time makes visible to the human agents the ways in which their memories are saved and shared around the network as a whole.

The physical constraints of the Park infrastructure meant that any device deployed for the project had to be self-powered, leading to the decision to use self-contained low-energy Bluetooth beacons to prompt interactions. Whilst we have outlined the problem of defining IoT precisely above, it is arguable that low-energy Bluetooth beacons are not, strictly speaking, IoT devices: they do not collect sensor data (other than device telemetry), and being for the most part 'broadcast only' devices, are not networked with one another [19]. However, they provide a way of prompting an interaction with a digital system that ties it to a specific object or place, allowing the creatures to behave in a fashion analogous to a network of IoT devices, and, moreover, allowing the process of data collection and the connections between that data, locations, and devices to be revealed to the user.

The use of these proxies and other trade-offs are crucial for this and other in-the-wild deployment designs because they serve two purposes: they are what allow such studies to take place, and at the same time disclose the limit on what can be discovered through them. Because the ethics of what we can do with these technologies, what uses they should be put to, and by whom, are currently up for debate, we cannot address them directly in a way that is acceptable for an in-the-wild study of this nature. There is therefore a clear disconnect between the capabilities of IoT technologies to collect, analyse and share data in ways which people may find counterintuitive or unaccept-

able, and the limits of what we as researchers can practically and ethically do to understand behaviours around this through an in-the-wild deployment. To frame the problem succinctly, how do you conduct in-the-wild research about data privacy practices in a public place without in the process violating the privacy of the public?

5 Conclusions

Tales of the Park was specifically designed to explore how people understand the privacy, security, and trust issues associated with networked technologies. By highlighting aspects of our engagement with our host organisation, we wish to demonstrate that the research team have had to negotiate precisely the ethical questions that currently animate debates around the proliferation of these technologies. As Ben Edmonds puts it, for both the Park itself and and its audiences:

"IoT, smart cities: they're terms that most people aren't familiar with, so the first thing for me is that most people don't even understand what this technology is, even in its most fundamental aspects. [T]hey want to know, 'what is it? How is it interacting with me and my technology?' The second thing, going back to data protection and the safety of their own personal information, I've found that a lot of people compare IoT with their day-to-day experience of telephone service providers and social media, so when they have experiences [that] things like Facebook are picking up things behind the curtains on what their interests are, what they potentially might buy and then relaying that back as advertising, theres an assumption that [...] with an IoT device, that capturing of information could be happening as well."

The Park are rightfully very careful that they do not (and are not seen to be) collecting unnecessary information about people, and are cautious about deploying technology that people might find difficult to understand. The negative issues that Edmonds cites above - data privacy, the potential for data analytics to influence people's behaviours, and the potential intrusiveness of IoT technologies - are precisely the research areas that Tales of the Park sought to investigate. Yet because we were deploying this technology in a public place with wide-ranging responsibilities to its various stakeholders, our capacity to directly address these issues was curtailed.

This points to a particular quandary for future HCI research around IoT. These technologies have the capacity to cause widespread changes in behaviours and social practices, and the likelihood is that actors with fewer ethical scruples than universities and public sector organisations will deploy them without fully exploring their negative impacts. We are therefore faced with a question of whether in-the-wild methodologies of the type used for Tales of the Park are capable of enabling researchers to understand these processes. Research is by its nature retrospective: we can only study what already exists. Yet the problem with IoT, and indeed with trends within networked computer technologies more broadly, is that they are developing and changing people and social structures far more quickly than either academia can study or regulators act. By developing and studying technology in-situ, in-the-wild methodologies seek to address this problem through the speculative development of a technology so as to discover what it might or could do, and the effects it could have should it become widespread. These methodologies therefore almost certainly have a part to play in research in the IoT space in future. Yet the fact remains that the initial research objective of Tales of the Park - to discover how people might react to 'rogue' devices in the public realm and the risks that this might entail - remains largely unanswered. This problem still exists, and will no doubt become of genuine concern as IoT technologies proliferate. Yet it is likely - as with the aforementioned examples of the 'Cayla' doll or Samsung's 'smart' televisions - that the full ramifications will only be discovered after the fact.

Our experiences on Tales of the Park, however, perhaps point to a possible way forward. The necessity for us to find proxies for 'real' data has parallels with the 'serious game' design approach: the use of play, usually (but not exclusively) understood as occurring in virtual space, to prompt engagement and reflection on a problem or issue, or as an educational tool [20]. Serious games have been designed to address a range of problems, from creativity as a therapeutic practice amongst dementia sufferers [21], to assist people on the autistic spectrum with understanding the emotional states of others [22], or to explore the ethics of global fashion production [23]. They can therefore be used to help people to explore social, ethical, and political problems.

The difficulties that people have in understanding IoT technologies and the scale of its potential ramifications are such that arguably there is value in pursuing serious game methods to help people explore them. We would suggest, then, that in-the-wild methodologies do have a part to play in this space, but not for their traditional purpose; namely the discovery of what affordances technology offers to solve real-world problems. Instead, we suggest that combining serious game design approaches with in-the-wild methodologies might enable us to use those affordances themselves as a springboard for thinking and debate about the nature and future direction of IoT technologies.

Acknowledgements

We would like to thank the London Legacy Development Corporation, Queen Elizabeth Olympic Park, and its associated venues and partners for hosting Tales of the Park. We gratefully acknowledge a grant from the Engineering and Physical Sciences Research Council which enabled this study to go ahead. The OpenBeacons platform on which Tales of the Park ran was funded through the Google Internet of Things Research Technology Awards Pilot study, who donated the Eddystone beacons used for this research.

References

[1] Y. Rogers, "Interaction Design Gone Wild: Striving for Wild Theory," *interactions*, vol. 18, pp. 58–62, July 2011.

[2] Y. Rogers, K. Connelly, L. Tedesco, W. Hazlewood, A. Kurtz, R. E. Hall, J. Hursey, and T. Toscos, "Why It's Worth the Hassle: The Value of In-situ Studies when Designing Ubicomp," in *Proceedings of the 9th International Conference on Ubiquitous Computing*, UbiComp '07, (Berlin, Heidelberg), pp. 336–353, Springer-Verlag, 2007.

[3] C. Golsteijn, S. Gallacher, L. Koeman, L. Wall, S. Andberg, Y. Rogers, and L. Capra, "VoxBox: A Tangible Machine That Gathers Opinions from the Public at Events," in *Proceedings of the Ninth International Conference on Tangible, Embedded, and Embodied Interaction*, TEI '15, (New York, NY, USA), pp. 201–208, ACM, 2015.

[4] A. F. gen. Schieck, H. Schndelbach, W. Motta, M. Behrens, S. North, L. Ye, and E. Kostopoulou, "Screens in the Wild: Exploring the Potential of Networked Urban Screens for Communities and Culture," in *Proceedings of The International Symposium on Pervasive Displays*, PerDis '14, (New York, NY, USA), pp. 166:166–166:167, ACM, 2014.

[5] L. Vent-Olkkonen, A. Lanamki, N. Iivari, and K. Kuutti, "It's a Pain in the... Wild?: Struggling to Create Conditions for Emerging Practices in an Urban Computing Project," in *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*, NordiCHI '16, (New York, NY, USA), pp. 51:1–51:10, ACM, 2016.

[6] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, Oct. 2010.

[7] B. Sterling, *Shaping Things*. Cambridge, Mass. ; London: MIT, 2005.

[8] P. N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven: Yale University Press, 2015, 2015.

[9] S. Greengard, *The Internet of Things*. MIT press essential knowledge series, Cambridge, Massachusetts: MIT Press, 2015, 2015.

[10] K. Morley, "Amazon Echo rogue payment warning after TV show causes 'Alexa' to order dolls houses," *The Daily Telegraph*, Jan. 2017.

[11] BBC, "Not in front of the telly: Warning over 'listening' TV," Feb. 2015.

[12] P. Oltermann, "German parents told to destroy doll that can spy on children," *The Guardian*, Feb. 2017.

[13] I. Shklovski, S. D. Mainwaring, H. H. Skladttir, and H. Borgthorsson, "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, (New York, NY, USA), pp. 2347–2356, ACM, 2014.

[14] A. Greenfield and M. Shepard, *Situated Technologies Pamphlets 1: Urban Computing and Its Discontents*. The Architectural League of New York, May 2011.

[15] "Wifi Data Trial - Understanding London Underground Customer Journeys," Nov. 2016.

[16] E. Ruppert, D. Bigo, and E. Isin, "Data politics," *Big Data & Society*, vol. 4, p. 2053951717717749, Dec. 2017.

[17] B. H. Bratton, *The Stack: On Software and Sovereignty*. Software studies, Cambridge, Massachusetts: MIT Press, 2015, 2015.

[18] "Facts and figures," 2017.

[19] A. McEwen and H. Cassimally, *Designing the Internet of things*. Chichester: Wiley, reprinted with corrections ed., 2014.

[20] I. Bogost, *Persuasive games: the expressive power of videogames*. Cambridge, Mass. ; London: MIT, 2007.

[21] A. Sisarica, N. Maiden, D. Morosini, L. Panesse, K. Pudney, and M. Rose, "Creativity Support in a Serious Game for Dementia Care," in *Proceedings of the 9th ACM Conference on Creativity & Cognition*, C&C '13, (New York, NY, USA), pp. 349–352, ACM, 2013.

[22] C. T. Tan, N. Harrold, and D. Rosser, "Can You CopyMe?: An Expression Mimicking Serious Game," in *SIGGRAPH Asia 2013 Symposium on Mobile Graphics and Interactive Applications*, SA '13, (New York, NY, USA), pp. 73:1–73:4, ACM, 2013.

[23] L. Gardner, "World Factory review - interactive play smartly unravels fashion industry," *The Guardian*, May 2015.