Exploring Physical and Digital Identity with a Teenage Cohort

Lia Emanuel
CREATE Lab,
Department of Psychology
University of Bath
Bath, BA2 7AY, UK
+44 (0)12253 83137
L.Emanuel@bath.ac.uk

Danaë Stanton Fraser
CREATE Lab,
Department of Psychology
University of Bath
Bath, BA2 7AY, UK
+44 (0)12253 86023
D.Stantonfraser@bath.ac.uk

ABSTRACT
The way we develop, use and visualize identity is rapidly evolving as research moves towards the capability to accurately link our digital and physical identities. With teenagers at the forefront of this hyper-connected world, this paper uses a systematic approach to contribute an in-depth understanding of teenagers' attitudes, values and concerns on privacy and identity information when considering both online and offline spaces. Using participatory design methods, we present three interactive workshops examining participant's perception of how their own online identities translated to the physical world, and the values and social considerations they hold around new or near-future identification techniques. We discuss how our deeper understanding of this age group's attitudes, values and concerns can be applied to designing socially acceptable identification technology and effective education on privacy and identity management among teens.

Categories and Subject Descriptors
H.5.m [**Information interfaces and presentation (e.g., HCI)**]: Miscellaneous, K.4.2 [**Computers and Society**]: Social Issues.

General Terms
Human Factors, Design

Keywords
Teenagers, participatory design, values, identity, privacy, social acceptability

1. INTRODUCTION
Teenagers are spending more time than ever sharing information online [20]. This age group, often referred to as Digital Natives [23], is increasingly relying on online social network platforms to maintain and strengthen their social lives, as well as develop relationships [20]. Simultaneously, the increased availability of technology is enhancing their ability to represent who they are across both online and offline environments in novel and innovative ways [16]. Importantly, these current trends among teens' use of networked technology are predicted to be driving factors in how this group and the wider public will perceive and use identities over the next 10 years [8]. There is a rich history of research on the concept of identity e.g. [4]. However, our perception and presentation of identity, or 'who we are', is rapidly changing [24]. We have the ability to represent multiple identities across both offline and online environments. Further, pervasive technologies have given us the capability to seamlessly move between these physical and digital personas. Therefore, it is unsurprising that we are now seeing new identification technologies and frameworks which incorporate this concept of identity existing across the physical and digital world [5, 25, 26]. As we advance to more sophisticated and novel ways to understand identity it is important to acknowledge not only how individuals use identity information, but also their values relating to how their identity information is used by others.

The IDC community has recently pointed out teenagers are one of the least understood user-groups [22, 33] in terms of understanding their distinct values and needs around the design and use of emerging technologies and online capabilities. We argue these developments around identification tools have implications for privacy and identity management among teens; the most likely demographic to be early adopters of technologies that will attempt to bridge the gap between the online and offline environments.

As part of a larger project, SuperIdentity [27], we report our work using participatory design to provide a richer understanding of the attitudes, practices and values teenagers place on their identity and privacy when online and offline spaces are considered a linked and unified environment. We first discuss the changing face of identity and privacy issues in relation to teenagers. We then describe how our approach of engaging with a teenage cohort over an extended period of time contributes to a more in-depth understanding of this age group's current values and expectations when they view different facets of online and offline identities becoming intertwined. We conclude by discussing how long term engagement with teens can lead to a co-design partnership in which the attitudes, values and concerns voiced in the current paper can be applied to designing socially acceptable identification technology, as well as raising awareness for good privacy and identity management practices among teens.

2. BACKGROUND
Modern identity takes on many facets. We refer to identity as defined by Saxby and Knight [24]; identity includes unique physical attributes such as biometrics, more biographical or descriptive characteristics such as our name, date of birth, and what cities we have lived in. In addition, identity includes personality attributes and behavior patterns. However, all of these facets of identity now also exist and represent who we are in the

IDC'14, June 17-20 2014, Aarhus, Denmark.

digital world, along with unique digital attributes of identity, such as an email or IP address. How this wide range of personal information gets presented (e.g. identity management) and to what type of audience (e.g. private to public) is rapidly evolving as we accrue more digital identity data e.g. [8, 25].

Considered 'digital natives', teenagers spend the most time online, are more likely to disclose a wider variety of personal information online [7], and have the highest uptake of networked mobile technology usage [17] relative to any other age group. This all feeds into a unique mixture whereby teenagers conduct their social lives fluidly moving between online and offline interactions [16, 23]. However, much of the research examining teenagers' attitudes towards and use of identity has been anchored purely in the social navigation of online network spaces [2] or how they conceptualize privacy and security in online spaces only [6]. For a group whose reality is so immersed in the digital world [10, 23], it remains unclear if teenagers value and use identity attributes similarly across online and offline interaction spaces.

Considering online spaces in isolation, research suggests teens show a relatively high degree of awareness in the importance of identity and reputation management, and do take steps to protect their privacy [1, 2]. Work examining e-safety education initiatives has shown methods such as fear tactics, blocking online access, and techniques aimed at children (e.g., cartoons) have had limited success in delivering e-safety messages or having any impact on the behavior of teenagers [1, 6]. On the other hand, peer led e-safety programs have been shown to be effective [1], and may be a more suitable method considering teens tendency to seek online privacy and identity management advice from friends rather than adults, such as a parent or teacher [21]. However, our current knowledge with regards to teenagers' values and attitudes towards sharing information and privacy practices in online settings have largely been limited to survey and one-to-one interview techniques [2, 6, 20]. A more systematic and in-depth approach to understanding 'digital natives' values, attitudes, and behavior towards identity management and privacy is now more important than ever with personal information being increasingly collected and collated across online and offline environments.

Consumer awareness around how companies sell seemingly innocuous personal information to 3rd parties or tracking browsing behavior for advertising purposes has received recent attention [19]. Teens in particular report some of the lowest awareness, to disbelief, that companies or 3rd parties may use their personal information [20, 7]. Research initiatives are also constructing increasingly sophisticated identification frameworks [25, 27]. The SuperIdentity Project is one example of ongoing interdisciplinary research exploring how associations between identity attributes across both the physical and digital world can be connected and/or predicted via a model of identity [26]. In modeling identity we consider known facts about an individual, such as gender, job description, blog content etc. It is often possible to infer new facts from the known set; these inferences can be modeled as new links between facts about that individual [10]. For example, if a person's real name and employer are known, we could infer their email address with a certain level of confidence. By considering a breadth of identity measures across a range of domains – biographic, biometric, cybermetric and psychological – it is possible to bring together a core *SuperIdentity* [26], linking facets of identity across its many digital and physical world dimensions.

The applications for such an identity model could benefit end-user groups, such as law enforcement and intelligence, in improving the capacity to make an identification decision and reduce identity-related crime and fraud. However, of equal importance is the social acceptability, wider attitudes and concerns regarding the use of identity within such a model, which is where our interest lies. Especially in dealing with sensitive personal information, it is important that the design and the capabilities of identification systems are seen as socially and ethically acceptable to ultimately be usable [15].With teenagers at the forefront of those who are hyper-connected and straddle the digital-physical divide [8], we are working with this age group to better understand the social impact of these research driven identification techniques.

In this paper we report the process and results of three workshops which focused on participatory design, specifically value-sensitive design: a systematic approach to designing for human values in technology [9], with a cohort of teenagers. We suggest value-sensitive design methods are the ideal next step in better understanding not only teenagers' attitudes and concerns around identity and identity management in this rapidly changing landscape, but also how this trend may affect the way in which teenagers utilize and interact with technology. In addition, the highly interactive, 'hands on' value-elicitation approach reported has shown to be successful in fostering engagement and in-depth discussion with teenage groups [28, 29], and effective in its peer guided nature [1]. The purpose of these workshops was to better understand teenager's attitudes, values and concerns on privacy and identity information if online and offline spaces are considered a linked and unified environment. Similar to the approaches taken by Woelfer [31] and Yoo et al. [34] we used a combination of value-elicitation methods, both qualitative and quantitative. Each workshop used a different design activity, involving a mixture of sketching, avatar design, and verbal scenario techniques. Although the qualitative workshop data was our primary focus, survey data was taken to enable a mixed methods approach allowing the quantitative survey data to enrich the themes emerging from the design workshops.

The workshop activities allowed us to explore participants' perceptions of their own online identities, both in social network settings as well as in visual form, and how they perceived these identities translated to the physical world. We followed this up by asking the cohort to brainstorm and design new technologies that would allow them to dictate how they would represent and possibly bridge their offline and online identities.

The first workshop used a variation of the mapping method developed by Panteli et al, [18] which provided a metaphoric perspective for how participants interact and share information online by layering their experiences on a physical environment. This sketching exercise encouraged group interaction and discussion about identity in a way which aimed to draw out perceived contrasts, parallels and overlaps between online and offline interactions. This provided insight into how this age group views identity in different contexts and situations.

The second workshop used avatar design, a user made representation to interact in online or virtual environments, in which participants created their own avatar and evaluated a peer's anonymous avatar. The aim of this task was to see what identity information participants could gather from their peer's avatar. Unlike sharing photographs, the participants had complete control in providing as much or as little information about their true physical features in the avatar platform. Although there is a rich literature on identity and self-representation via avatars, including adolescent specific user groups, e.g. [12, 14], we were particularly

interested in attitudes on the possibility that avatar designs may provide links to other forms of identity information. This workshop's method enabled us to explore both values and behavior around the choices this group makes sharing visual information online about their physical identity.

The third workshop used sketches and verbal scenario creation in which participants were asked to design new forms of future identification methods and technologies. Participants' designs acted as the value-elicitation to better understand the identity attributes and identification techniques this group was aware of and to articulate their values and social considerations around new or near-future technology. It is worth noting, we did not use these design activities as a means towards developing or designing 'solutions' for identity and privacy across digital and physical domains. Rather we used the design workshops as a way to facilitate an in-depth discussion with our teen cohort to gauge values, attitudes and concerns about identity information and privacy across online and offline spaces.

3. METHOD

3.1 Participants and Data Collection Context

Thirty-one students participated in the project, encouraged to take part in all three workshops (approx. 55% participated in all three). Students were recruited from two schools in the South West, UK; aged 13-18 years old. All participants provided informed consent to take part and parental consent was attained for participants under the age of 18. Participants were recruited by circulating fliers through contact teachers at each school for an ICT afterschool activity group being held bi-monthly. The workshops were held at the schools, within classrooms familiar to the participants and in similar year groups (e.g. no more than a 2 year difference in each group). A teacher was present to help gather the participants to the appropriate classroom before leaving the researcher to introduce and start the workshop activity. As an incentive for continuing participation across the project, a points scheme was used in which participants accrued points for each workshop attended and could trade these in for a £10 gift card.

3.2 Procedures

Three different workshops were run at each school during December 2012 - June 2013. The workshops consisted of a brief introduction explaining the activity an related instructions. In workshops involving drawing (1 and 3), participants worked around large tables, organically forming groups of 2-5 people but also in close enough proximity for groups to interact with each other. Each group was given large sheets of paper and color markers, spending approximately 30 minutes engaging in the drawing/designing activity. In workshop 2, the avatar design activity was held in computer classrooms, with participants working individually during the design portion. At the end of each design phase, the researcher led a 30 minute semi-structured discussion exploring concepts of identity and privacy in relation to participants' final designs and their design process. All workshops were audio recorded to capture participants' dialogue during the design activities and the semi-structured group discussion.

Following the first workshop participants were given access to a 2-page online survey to complete outside of the workshops over the course of the project. This survey collected additional information about the cohort's attitudes, practices, concerns and strategies around privacy and identity in online and offline environments. Survey questions included both discrete questions (e.g., on average how many hours a day do you spend online?) and scale rated questions (e.g., on a scale of 1, very rarely, to 5 very frequently; how often have you found that comments made online go beyond your intended audience?) as well as open ended questions (e.g., how do you feel about the use of CCTV?).

During the first workshop participants were asked to use markers and large sheets of paper to draw a floor plan that depicted how they visualize online social network sites (SNS) using a familiar physical environment (e.g. school, shopping center). While drawing their floor plan participants were encouraged to discuss and develop ideas with their peers. Participants were also asked to consider features they use in SNS and how they may map on to their floor plan, labeling what they thought was similar or different between the online and offline social spaces.

In the second workshop participants were told they would be creating an avatar anonymously. After designing their avatar, they were told they would be given a peer's avatar to analyze to see what identity information could be derived from the avatar. Prior to creating their avatars, participants were asked to fill out an abbreviated version of the Interpol Anti-Mortem form for missing persons (AMForm) [11] shortened to pertain to the avatar platform, *Voki Classroom* [30], which was used. Participants completed the form to best describe 17 of their own physical features. Following this participants were given approximately 20 minutes to create an avatar, being asked to create what they believed best represented who they are. Participants then used an identical AMform to describe 17 features of a peer's avatar (who remained anonymous). Finally participants were given the AM form of their avatar completed by a peer to compare against the AM form they filled out to describe themselves.

During the third workshop participants were asked to design new forms of identification (ID) that could be implemented in the future. The researcher began the workshop asking participants for examples of ID they may use, drawing attention to both online and offline forms of identification (e.g. passport, driver's license, usernames) and authentication (e.g. passwords to email/facebook accounts, PIN numbers). The researcher also introduced examples of near future technology being developed (e.g. face recognition on smartphones, RFID implants, inferred gait mapping) that used a wider array of identity attributes. Working in groups participants were asked to design an ID for the future and consider what type of personal information would be important to include, how their IDs would function, and how they would secure their personal information.

3.3 Analysis

All workshops were audio recorded and transcribed. The materials the participants created during the workshops, the transcribed discussions during design phases, the semi-structures discussions and the responses to the open-ended survey questions were analyzed using thematic analysis [3].

4. RESULTS

4.1 Mapping SNS

From the first workshop, a total of 10 map drawings were created. All groups used either areas of their school, such as a student common room, or their house as their physical space. We discuss the themes around teenagers' use of and attitudes towards identity across online and offline spaces that emerged from the drawings

themselves, the in-depth discussion that was facilitated by the mapping exercise, alongside the participant's responses from the online survey.

4.1.1 Diversity of Socializing Spaces

The drawings of familiar physical spaces brought out the numerous different ways teenagers interact face-to-face. Sharing a secret with one person, organizing a group of people to meet up after school, or showing friends photos were common across many of the drawings. However, through layering how these interactions parallel to activity on SNS, participants revealed the diversity of SNS they use. Fifteen unique social interaction platforms were cited or labeled on drawings as being used by participants in the workshop. What this group defines as "SNS" encompasses a number of different interactive platforms, not just one or two different main stream networks (e.g. facebook, twitter). It became clear that participants use many different social platforms, such as private messaging applications (e.g. BBM, Kik), organizing meeting places (e.g. Foursquare), and sharing visual media (e.g. 4chan, YouTube) to fulfill very different facets of sharing information and interacting with people. The use of a variety of SNS appeared to allow participants to enjoy a diversity of interaction that more closely mirrored the choices they have to share information face-to-face.

Through drawing physical boundaries, rooms and arrangement of furniture to compartmentalize communication in a tangible physical space, it became apparent that this group similarly perceived different networks and online features to offer varying levels of privacy based on the target audience for participants' information. For instance, small confined spaces such as the toilets or small corridors were paralleled with private messaging, whereas large communal spaces were aligned with facebook wall posts (see Figure 1).

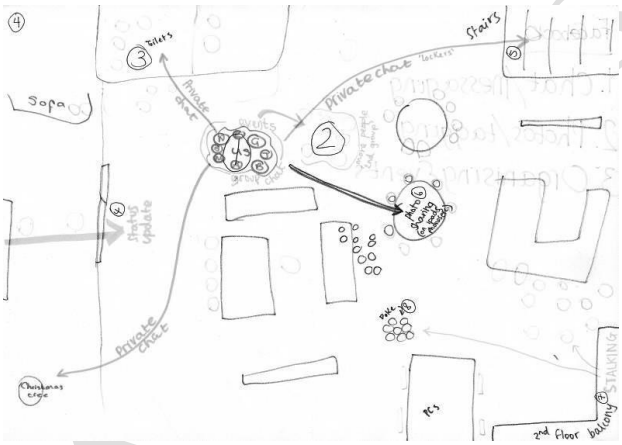

Figure 1. Drawing from one group who used their student common room to map out SNS

One group described how they organized social networks within their house as having Skype as their bedroom, because it is generally used for more private conversations and YouTube in their living room since it is more public and more people will see what you post or say. Similarly, awareness of the type of audience within certain networks was depicted, with an image sharing social network as the bathroom because, "*It is full of trolls that's why it is in the toilet*".

However, both physical and online spaces were not perceived as similar with regards to the level of control the group felt they had over the privacy of personal information once provided online. The majority of participants voiced the opinion that they felt that information had more permanence online, with one participant summing up the discussion by saying, "*offline people just chat and it's done. If it's not [online], it will eventually die out. When it's online it's there for everyone, you can't delete it*." Similarly, responses to the survey supported the beliefs drawn out of the group mapping exercise, with participants feeling they had slight to moderate control to delete or change personal information once posted online (rated M = 2.60, SD = 1.01), on a scale anchored 1, not at all, to 5 very much so.

4.1.2 Social Value

The majority of the physical space drawings included the labels of friends' names, and depicted people generally interacting in small groups. When asked to expand on what the group thought was similar and different about how they approach or get to know others online and offline, the majority of participants stated they primarily contacted and interacted with individuals on SNS that they knew offline. The main value of having an identity or presence on SNS to this group was largely toward the benefit of their face-to-face offline social life. In the online survey, socializing online was rated as the second most important online activity behind surfing/browsing and ahead of downloading media content. This was elaborated on in the workshop, with several participants stating their SNS presence was important for organizing, being included in social events and activities happening offline with known friends. The passive consumption of other's information was also highlighted as a unique facilitator of face-to-face interaction, "*I think it [SNS] does really help with communication, like sometimes it's easier to talk to someone if you know what they are into.",* and, *"snooping, looking things up about people is like my primary reason for using facebook".* This view raised in the mapping exercise was also evident in the survey with participants reporting spending significantly more time (once a day) passively checking content on SNS, relative to actively contributing information (once a week), $t(13) = 4.69$, $p < .001$. Our teen cohort was very aware that how they represent themselves on SNS platforms bleeds into their offline social lives, and state that maintaining a similar digital persona to their real-world persona actually benefits their social exchanges and relationships.

However, friends were also perceived to be the biggest threat to unintended sharing of personal information in online settings – a feeling that was not as prevalent in offline settings. During the workshop, through discussing how they compartmentalized interactions in their physical space participants were able to expand on concerns about control of personal information online and offline. Participants generally felt that they were fairly good at being careful about who they share potentially sensitive information with, but that 'friended' people who have access to their profile information, for example, were more likely to overshare their information. Further, the diverse SNS engaged with by this cohort was not seen to offer privacy protection in this instance, with overlapping networks of friends and the increasing emergence of services that link together different SNS accounts, making it more difficult to compartmentalize information online. Participants acknowledged this type of spread of information through friends was possible offline (e.g. "*overheard conversations*", "*gossipy friends*"). However, there was far less attention and discussion about the control and

compartmentalization of personal information offline, suggesting this is less of a concern within the cohort.

4.1.3 Blurring Digital and Physical

Within participants' drawings there was one key aspect that appeared to blur the physical-digital divide. The majority of the physical environments utilize networked, often mobile, technology to depict how participants communicate with others. For instance, communicating via tablets and smartphones in participants' physical environments was depicted as a parallel with private messaging in online platforms. Similarly, one group drew talking with friends on Xbox live in their living room by microphone as a physical environment equivalent to group chat in online SNS. The prevalence of these devices being perceived as comparable forms of interaction in both physical and digital environments, suggests ubiquitous technology is one important facilitator in the blurring of cyber and physical spaces among teens.

However, there were some areas of bridging digital and physical spaces which were seen as concerning within the group. In discussing how the group perceived different levels of privacy, there was a pervasive feeling that anything placed online was going to be highly accessible to others. For instance, one participant stated: "*online just typing someone's name into google, their facebook account or any other account just pops up. You can easily access information about them. But in real life you just can't do that*." However, the biggest concern about this level of access to personal information centered on the ability to link physical-base information, (e.g. a phone number or current location) to a cyber-persona (e.g. username or email address). This concern was echoed in the survey, in which 61% of responses to participants' biggest concerns regarding personal information online were specifically related to unknown individuals obtaining or misusing location, demographic and contact information. When posed the same question about offline environments, concern on the misuse of information (47% of responses) was lower and more generalized (e.g., "*personal information*", "*my information*") rather than specified to location or demographic details. This suggests attributing physical-based information to a cyber-persona is seen as less acceptable than attributing cyber-based information to a physical world persona by this cohort.

4.2 What Does Your Avatar Say About You

In this workshop, 15 avatars were created and analyzed by the cohort. When discussing how they approached the process of creating their avatar the majority of participants stated that they tried to make their avatars as similar to their actual physical features as they could. For instance, none chose to portray themselves with physically impossible features (e.g. purple skin or elves ears), none changed their gender, and very few changed distinguishing features such as hair color (23%) and eye color (7%). In fact, these types of characteristic features, such as hair, eyes and mouth were cited by participants as aspects they spent the most time on to get "just right" in relation to their actual features: "*Oh wow [participant name], yours looks just like you! It's the hair that gives it away*". Likewise, participants were generally unsurprised by the similarity between their own self-reported features on the Interpol AM form and those of their avatar's that were rated by a peer. Indeed, using Kappa coefficient [13] to determine if the agreement on the ratings of self and avatar features exceeded chance levels showed there was significant agreement for 77% of participants (all significant values $K \geq .44$; $p \leq .001$). Interestingly, the 33% who did not show similarity in self-avatar ratings above chance levels created avatars with highly stylized, cartoonish features, as opposed to more realistic features (as in Figure 2).

Figure 2. Example avatar from workshop

That is not to say exploration of different physical features didn't happen. Several participants described their avatar design process as testing out different looks, exploring the features and functions of the avatar platform, before trying to find features that were a more accurate portrayal of themselves. For instance, one participant said they spent about half their allotted time flipping through and 'trying on' features before "*entirely scraping that avatar*" to create their final more realistic avatar. When asked what features participants felt they were more creative with or deviated from their appearance, several stated more general alterations such as, "*I wanted to look a bit more cartoony*" and "*I made myself unbelievably good looking*". One participant highlighted there was a social benefit in creating avatars that more closely resembled their appearance: "*I have like 6 different avatars for different things but I keep them pretty similar [to me] so my friends know it's me*". Further, participants seemed to project this design approach onto the wider public, stating under certain circumstances they would trust the accuracy of an avatar as a reflection of its creator: "*If the avatar isn't unbelievably crazy looking…[it's] probably pretty spot on*".

However, there was a general feeling of skepticism that participant's avatars would provide valuable identity information to unfamiliar or unknown individuals online. For instance, participant's suggested that in the workshop exercise being in the same room and able to see who potentially created the avatar they were rating was an advantage they would not have just seeing an avatar online. Even when prompted further about aspects incorporated in their avatar that were not based on their physical features there was little concern around how that may relate back to them as a person. For example, one participant said they spent a lot of time choosing their avatar's clothing to include their favorite color, while others felt they spent a lot of time choosing a background picture to relate to their interests. Although the cohort agreed that aspects of their avatar design could link to other aspects of their identity or persona, many voiced the feeling that information regarding their interests was not particularly unique and could not be used to identify who they were offline.

4.3 Designing Future Identification Methods

The third workshop asked participants to consider what types of identification (ID) they could see being implemented in the future. In this type of future design scenario the cohort took a very imaginative view on the identification process. However, a number of underlying themes in this group's awareness and

opinions of identification practices emerged. We briefly describe the five final ID designs the cohort created, before discussing the themes which came out of the design process, the group discussion and responses from the online survey.

4.3.1 The ID Designs

First, personalized tattoos were suggested in which the wearer could scan different tattoos made with traceable and irradiated ink (so they could be scanned through clothing). These tattoos would provide relevant identity information across different situations. The tattoos were described as unique to the individual with everyone having a personalized combination and style. The designers suggested the tattoos could also be made out of invisible ink to obscure patterns to the naked eye as a privacy measure.

Second, was the BeID system. The designers described the scenario that when an individual needed to be identified a micron-sized robot bee would 'sting' them, collecting their genetic information. The sample would then be taken to a centralized information center which matched the individual's genetic data to all other collected personal information on file. Notably, this group did not specify any privacy or security features for their identification system.

Third, a tongue sensor was designed as a personal security authorization method. The designer gave the example of access to a mobile phone, whereby the owner would lick their phone and the tongue scanner would pick up that person's unique tongue patterns to unlock the phone. This was the only design based on authorization. It held no identity information per se (e.g. you are either the correct individual or you are not), but potentially authorized access to further personal information on an individual's phone.

Fourth, the 'Hipster glasses' (Figure 3) were described as allowing the user to see detailed personal information on the lens of a pair of glasses about another individual. The glasses used facial recognition to identify a person and bring up all of their publicly available information. This group detailed certain settings that would authorize, via iris scan authentication, the wearer to receive more detailed information. For instance, a doctor could have access to a person's medical history, a police officer could access criminal history or a personal trainer could access a person's diet, weight and activity levels.

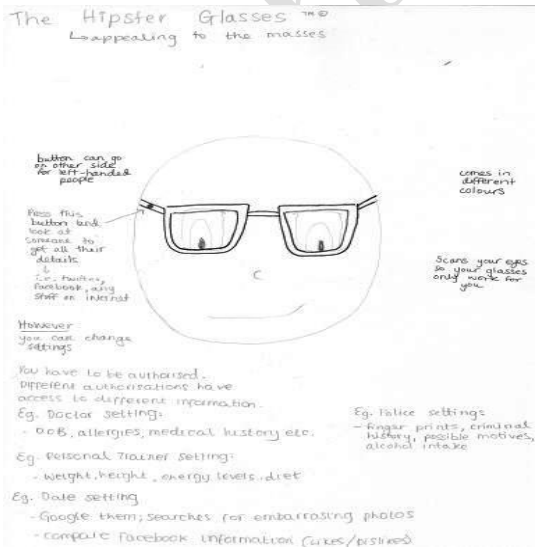

Figure 3. Hipster Glasses ID design

Last, ID jewelry was presented in which a chip and memory card was hidden within a piece of jewelry that would contain all of an individual's identification information. The user would scan the jewelry and provide a password or retina authentication to access and bring up necessary identity information. This group included a number of traditional security features, such as a small locking mechanism for the jewelry, as well as more technological features. Namely, the personal information could only be accessed if it was within a particular radius of the owner which was controlled by an RFID style chip implanted in the owner's tooth.

4.3.2 Biometric Focus

Throughout the design process and the group discussion participants viewed the use of biometrics as an obvious next step in the future of identification. Discussion of methods that would enable identification during the design phase was almost entirely on using biometric or biological means, such as blood sample, saliva, iris recognition, facial recognition and fingerprint scanning. Likewise, participants utilized biometrics as a security measure for accessing identity information. For instance, the ID jewelry and the Hipster Glasses relied on retina scanning to access information, and the Tongue scanner even introduced a new biometric in authorization via unique tongue patterns. The high frequency of biometric measures used in the ID designs echoes the positive feelings reported in the online survey when participants were asked how they felt about biometric measures being used for identification. All but one participants reported an accepting attitude, suggesting biometric identification was "*a good way to prevent fraud*" and "*made them feel safer*".

Participants also considered how more traditional tokens could be used in new ways or combined with biometric measures. In the initial design phase one group came up with an arm band that essentially turned the users arm into a USB stick when they needed to provide identity credentials. Another group suggested a smart card with the ability to hold a terabyte of information: "*Think if you could have like a terabit of information stored on your card, like your DNA sequence*". From the final designs, the personalized tattoos and the ID jewelry employed this token concept, whereby each could be scanned to provide identity credentials.

4.3.3 ID use across online and offline spaces

Across the five designs, participants reported relatively varied capabilities on how their ID designs could be used across both online and offline spaces. Both the BeID and the Tongue scanner designs were presented by the designers in a physical world setting, with no mention of online capabilities. When the larger group was asked if they could see the Tongue scanner technology being implemented in another broader ways only physical world applications were brought up, such as verifying identity at the airport. The designers of the two IDs that used scannable tokens, Personalized Tattoos and ID jewelry described scenarios where their designs could be used almost entirely in physical environments. Both design groups did agreed that the scanning properties could allow someone to log in to online services, for instance using their designed IDs in place of passwords. However, this online capability was online considered when directly prompted by the researcher. The Hipster Glasses design, akin to the concept of Google glass, was the only design presented in a way that relied heavily on matching identity based offline information (e.g. scanning facial features) to information related to that person online; "*You look at someone and press the button and then all their information comes up on the glasses. So on the*

normal setting you just get their twitter and facebook and anything [about them] on the internet."

4.3.4 Privacy: how and who can access information

In all of the presented designs dealing with identification, apart from the ID jewelry, identity information was not kept with the individual. In the ID jewelry, this feature was described as a means to secure personal information, "*obviously the bracelet could just stay [on your wrist] it wouldn't have to be removed, or very often anyway. It would be quite useful because it would be hard to lose… and disguised just as a normal piece of jewelry… so harder to steal*". In the BeID, the Hipster Glasses and the Personalized Tattoo designs the actual identity information about a person was described as being stored on an external database or systems. For instance the BeID designers described their process as, *"So then the point sort of stings you and goes to an Info Centre, like they take themselves to the Info Centre and all your information is there."* In these three designs, the means to access or link a person with that information is kept with the individual (e.g. genetic material, retina scanning, and permanent ink patterns), but the actual information about them is not. These three groups also took on a relatively distinct perspective for who was accessing this personal information.

Two groups, the BeID and the personalized tattoo designers, explicitly presented their identification methods from a government/law enforcement perspective. The irradiated nature of the tattoos was presented within the scenario of ease of capture on CCTV and surveillance equipment, "*but it would be easy to trace and scan, like CCTV could pick it up*". The BeID group made it clear who they envisaged operating their ID system when asked if someone tried to evade identification and smashed a bee; "*Then you owe the government millions of pounds*". Although the Hipster glasses were presented in the scenario of ease of access to information for the individual user, the design revolved around gathering information about others. The designers presented scenarios where individuals in an authority position could access more sensitive data; "*there are settings which you have to be authorized to get, such as the doctor setting…and a police setting*". However, the group did not elaborate on who decided authorization statuses or how an individual may protect their own information availability to others with these glasses. Participants responses to surveillance and identification techniques in the online survey mirror a similar level of acceptance as suggested through elaboration on their ID designs. When asked their feelings towards CCTV and related surveillance techniques, all participants were very positive about its current use. While 50% simply stated acceptance, 25% reported CCTV surveillance was beneficial if it was used appropriately, such as for legal or law enforcement purposes. A further 25% stated CCTV was valuable if used appropriately but did acknowledge feelings of discomfort, "*I think it is sometimes an invasion of privacy but it is there to keep people safe".*

4.3.5 Values and Barriers on the uptake of new identification designs

Through each group's presentation and explanation of their new IDs, the cohort as a whole was very vocal in expressing and discussing acceptance and discomfort around the proposed functionality of their peers' designs. Negative perceptions of using the new technologies and techniques for identification were not generally based on the protection or privacy of information. Rather, lack of acceptance of certain features was largely grounded on personal discomfort, both physically and socially. During the design phase some biometric measures, such as DNA extracted from blood and saliva samples, were discarded quickly because they were perceived as painful; *"you would have to cut yourself each time you used it [blood sampling]*" or unhygienic; *"you would end up spitting on someone [using saliva sampling]".* Socially normative behavior was also a driving factor in negative views on the implementation of some of the final designs. For instance, in the case of personalized tattoos one participant suggested tattoos were socially undesirable: "*Tattoos are definitely unattractive*". Similarly, discussing the tongue scanner brought up the view that an individual would "*look weird*" licking their phone in public, even if it was more secure than a password.

Two design features in particular stood up very well against unacceptable or uncomfortable authentication methods. First, the tongue scanner was met with resistance from the group due to its perceived socially awkward and unhygienic method of authorization. However, the scenario of securing mobile phones specifically piqued the interest of this group. With the majority (60%) of the cohort reporting owning a smartphone, personal devices were reported as being highly personal and private in the online survey. Second, the high degree of customization in the wearable IDs was of particular interest to the cohort. Much of the discussion around these types of designs was building on the creative aspects and how the group could tailor the IDs to suit their individual style or tastes. This customizable aspect led several to eventually accept initially perceived negative qualities (e.g. implanting an RFID chip in a tooth for the ID jewelry).

5. DISCUSSION

The value-sensitive design methods in the present paper provoked considerable reflection and discussion with our teenage cohort in the way they view identity across many dimensions. Both the mapping SNS workshop and the Avatar designing workshop contributed insight into participants perceptions of their own online identity – how they use those identities, how they value private and public availability of their identity information – and the facilitators, benefits and concerns around how these identities may translate to the physical world. The designing a future ID workshop provided a broader approach by offering our cohort a unique way to express their level of awareness, values and social considerations around how they could ideally represent their identity through a variety of identification techniques.

The importance of relationship maintenance and reputation management in online spaces for teens is well documented [2, 16]. However, asking participants to consider how they share information and personify themselves layered across both online and offline environments yielded several insights into their values and behavior, as well as concerns. The variety of online spaces utilized by our participants, each for a subtly different purpose, allowed them to enjoy a diversity of interaction that more closely mirrored the choices they have to share information face-to-face. Similarly, the use of many different online social spaces also afforded participants a way to compartmentalize their identity information. Different spaces were used as a means for controlling the flow of information and indicated a relatively keen awareness of the potential audience consuming that information. In a sense, this reflects a relatively nuanced approach to privacy e.g. [2]. However, the variety of online SNS this age group engages with also provides a very rich identity foot print which affords subtly different snap shots of that person (e.g., video, images, voice, and textual/content information). Importantly, this type of selective

sharing of information across diverse online platforms implies research can no longer be bound to just one main stream platform, such as facebook e.g., [35], to understand the full picture of how teens share or disclose identity information.

However even with using this compartmentalization strategy, participants felt there was a difference in their ability to control the privacy of their information online versus that ability offline. This feeling appeared to stem from two points. First was the permanence of personal information online, which was not present or perceived in offline disclosure. Second, participants' friends were seen as the biggest threat to teens' ability to control personal information. Both the qualitative and quantitative data suggested participants were highly confident in their ability to keep sensitive personal information private, across both online and offline spaces. However, it was primarily within online scenarios where friends and contacts were seen as more likely to 'overshare' participant's personal information.

Nonetheless, the social value or benefits gained among friend networks emerged as one of the main motivations for maintaining a similar digital persona to teens' physical persona. Similar to previous findings [20], our teen cohort reported that they primarily used online SNS to socialize with people they knew offline. In addition, participants were very aware of the high overlap in how they represented themselves online and offline among their friends. In both the mapping social networks and avatar workshops participants provided examples, such as improving face-to-face interaction or ensuring friends recognized them online, of the positive benefits they had experienced from keeping their offline and online self-representations similar.

Similar patterns of behavior were seen in the avatar workshop. The cohort's process of designing their avatar was creative but both the qualitative and quantitative data suggested the majority of the group created an avatar to resemble their actual features relatively closely. This is in line with McCue's [14] findings that adolescents showed a tendency to create avatars with realistic features as opposed to fantasy features. However, our findings uncovered an interesting contrast. Participants explicitly tried to design an avatar that accurately represented their appearance and were able to see that their peer's ratings of their avatar were quite similar to their own rating of their physical features. Yet, participants felt their avatars would not provide important or unique identity information in a public online setting. There was little to no concern voiced about the potential for an avatar representation online linking back to the participants offline. One possibility is that the greater control afforded to participants to be selective about the information related to their actual physical features led to lower levels of concern. Alternatively, the avatar platform used [30] was designed as a teaching aid to use avatars for teacher-student and student-student interaction on class assignments. Unlike other larger avatar platforms, such as Second Life, realistically the audience likely to see the participants' avatar was relatively small, and known to the participants offline.

However, this attitude was particularly interesting considering the tension brought up around the ability to link online and offline identity information. Overall, attributing physical-based information to a digital-persona was seen as less acceptable than attributing digital-based information to a physical world persona by this cohort. One example given by a participant was concern around the ability to infer and attribute physical based information (e.g. house address) to a digital-identity (e.g. email address) that was not expressly provided by the participant. This tension, which also emerged in the quantitative data, was voiced as a concern primarily due to the higher level of accessibility of personal information online versus offline.

The results suggest there is some tension around others ability to share or spread information from one online network to another. Particularly if this spread involves inferring physical world information, such as location or demographic details, and linking it to an online persona. However, participants were generally unconcerned that certain pieces of information could be derived from their avatar, such as interest, hobbies and general physical features. This may reflect the perception that some types of identity information are more or less sensitive than others. Yet it remains unclear how participants' attitudes and concerns may change when made aware of emerging identification techniques. The designing a future ID workshop began to address this question.

The envisioning aspect of the future ID workshop may have led participants to use design features that they found innovative or exciting, rather than reflective of their acceptance of such techniques were they implemented. For instance the BeID design is by no means realistic 'solution' for identification or identity management, nor do we believe the designs were necessarily seen this way by the participants themselves. However, this creative aspect of the participatory design activity did allow the group to articulate a number of values and attitudes they held around identification methods.

The cohort was very comfortable with using and creating new biometric indices. Biometric measures were the favored method among the group for both securing access to identity information as well as a means to identify an individual. The heavy use of biometric measures, almost an exclusively physical world identity attribute, may be one reason why all of the future ID designs apart from one were presented as functioning primarily in physical-world environments. On the other hand, the choice to maintain identity information in offline environments may further indicate tension around linking unique physical identity information to digital identities, and feelings of greater control of offline information that were voiced in the previous workshops.

We found teenagers also showed high usage of networked tokens, IDs working with existing surveillance practices and centralized identity databases (synonymous with dataveillance). This is in contrast with studies exploring adult user-groups. A relatively high level of resistance to ID methods incorporating government surveillance, dataveillance, and networked ID tokens has been documented among adult populations [32]. Within the present cohort, the wide use of these ID methods, biometric indices and the ease of discussing, largely the merits of, these techniques reflects some degree of acceptance. Teenagers are immersed in this type of technology, if not directly in their daily routine then through extensive media exposure, and therefore would perceive these methods as familiar or viable, unlike perhaps their adult counterparts [23]. However, the cohort's acceptance of these surveillance practices was largely dependent on the context in which it was used. For instance, if used for protection or by an authority figure. Future research needs to address values around privacy and identity management with this age group across a spectrum of contexts. A pertinent example which spans both online and offline spaces are teens' attitudes and concerns on the commercial (mis)use of identity. Likewise, values and trust around the concept of anonymity (e.g. the right to be forgotten,

[24]) has yet to be explored in relation to teens view of acceptable uses of identity and identification technologies.

The current results provide a platform to begin to understand teenagers' values and concerns on the use of their identity information in light of the rapid evolution of identification technology spanning online and offline spaces [25, 26]. Namely, the reported workshops provide situations relevant to this age group to frame further examination of teens' attitudes and acceptance around how their identity is used. Specifically, further understanding values on technology with the capability of taking what was seen as relatively non-unique identity information and collating, inferring, and linking to other aspects of their identity [27]. For instance, mobile devices were portrayed as a favored way for participants to share information and facilitated interaction across both online and offline contexts. However, touchscreen devices can reveal identity information about the user via swipe gestures, such as gender, age, and height [26]. Through extended engagement with the teenage cohort, this mobile device example can be used to introduce how identity modeling makes it possible to infer or predict new identity information from a known set of facts [10], within a context that is relevant to the cohort. In this way, the cohort moves from participant to co-designer by feeding back on the acceptability of deriving identity information through identity modeling techniques, as well as suggest design features to improve and address negative or socially unacceptable features.

This use of participatory design methods to engage with teens also has implications for improving e-safety education and practices. The hands-on, interactive design workshops were an effective way of sparking interest on the topic of identity with teenagers. Importantly, this method led to enthusiastic engagement and provoked animated discussions. Through the semi-guided activities participants were able to articulate amongst their peers the main values and concerns they held while debating and exchanging advice on how they tended to make choices about sharing and using identity related information. This approach in raising awareness around disclosure practices is more in line with teen's tendency to go to peers for advice [21]. Together with the flexibility of using different activities to address different and ever evolving issues on identity management makes value-sensitive design methods a potentially valuable tool for e-safety education. Future research would benefit from further evaluation among both teens and teachers on the impact value-sensitive design methods has on changing identity management and privacy practices.

6. Conclusion

Constantly evolving pervasive technologies allows us to develop and move between different physical and digital personas. This makes better understanding the fusion of digital and physical identity a key priority in how the wider public will perceive and use identities over the next decade e.g., [8].With teenagers at the forefront of bridging the online-offline divide, the current findings suggest a number of key attitudes, values and concerns regarding identity across physical and digital spaces.

There were three main areas where we found teenagers perceived and largely use online and offline personas in a continuous way. First, similarly across both spaces, this group develops, uses and shares personal information across numerous and diverse social spaces, each allowing them to share a subtly different, and an overall rich representation of themselves. Second, through primarily having similar friend networks online and offline there was social value in maintaining similar personas across both spaces. Third, mobile devices were portrayed as a favored way for participants to share information and facilitated interaction regardless of online or offline context. Networked mobile technology may be at least one artifact that blurs and provides the strongest link between teenagers' digital and physical identities.

In contrast, two main points emerged which may indicate future tensions regarding the fusion of digital and physical identity. First, new identification frameworks should carefully consider the capabilities and security around inferring and attributing physical-based information to digital personas when not expressly given by the owner of the digital persona. Second, the concerns voiced about the reduced control over and ease of access to identity information was largely seen as a tension felt in online spaces only. Future research would benefit from focusing on design features and technology which address this latter issue, which in turn may reduce the tension around linking physical information to a digital persona.

Building off of previous survey and interview based studies [6]; the participatory design approach used in the present paper provided a rich and more comprehensive insight into teenagers' perception, experience and behavior with regards to identity and identification technology. In addition, our methodological approach contributes to the less developed area of participatory design methods for teen-CI [33], as well as highlighting the potential for value-sensitive design approach as an effective e-safety awareness tool. We can now move forward, using these outlined areas of similarities and tensions around *SuperIdentity* as a platform to engage with teens as co-designers of socially acceptable identification technology while developing awareness and good practice in privacy and identity management.

7. ACKNOWLEDGMENTS

This work was supported by EPSRC Grant (EP/J004995/1 SID: An Exploration of SuperIdentity). Colleagues on this grant are thanked for their helpful contributions to the current work. The authors would also like to thank Duncan Hodges for his engagement with the user-group, the students and schools taking part in the workshops. We also thank those who reviewed earlier versions of this paper for their helpful feedback.

8. REFERENCES

[1] Atkinson, S., Furnell, S. and Phippen, A. 2009. Investigating attitudes towards online safety and security, and evaluating a peer-led internet safety programme for 14-to-16-year-olds. Retrieved April 4, 2012. http://dera.ioe.ac.uk/1451/

[2] boyd, d. and Marwick, A. 2011. Social privacy in networked publics: Teens' attitudes, practices, and strategies. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.*

[3] Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3:2, 77-101.

[4] Brubaker, R. and Cooper, F. 2000. Beyond "identity". *Theory and Society 29*: 1-47.

[5] Collaborative information, Acquisition, Processing, Exploitation and Reporting (CAPER): for the prevention or organized crime. *Retrieved August 25, 2013*. www.fp7-caper.eu/

[6] Davis, K. and James, C. 2013. Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology* 38:9, 4-25

[7] Eurobarometer 359 Special Report. 2011. Attitudes on data protection and electronic identity in the European Union. *TNS Opinion & Social and Directorate-General Communication*.

[8] Foresight Future Identities. 2013. *Final Project Report*. The Government Office for Science, London. Retrieved August 22, 2013. www.bis.gov.uk/foresight/our-work/policy-futures/identity

[9] Friedman, B., Kahn, P.H., Jr., and Borning, A. 2006. Value Sensitive Design and Information Systems. *In Human-Computer Interaction in Management Information Systems: Foundations*. P. Zhang and D. Galletta, Eds. M.E. Sharp Inc., New York.

[10] Hodges, D., Creese, S. and Goldsmith, M. 2012. A model for identity in the cyber and natural universes. *Proc. European Intelligence and Security Informatics Conference*. Odense, Denmark, EISIC'12, pp. 115-122.

[11] Interpol DVI forms (version 2002). Ante-Mortem (yellow) Victim Identification: Missing Person. *Retrieved Jan.15, 2013*. http://www.interpol.int/INTERPOL-expertise/Forensics/DVI-Pages/Forms

[12] Kafai, Y.B., Fields, D.A., and Cook, M.S. 2010. Your Second Selves: Player-designed avatars. *Games and Culture 5*(1), 23-42

[13] Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics* 33:159-174.

[14] McCue, C. 2008. Tweens avatars: What do online personas convey about their makers? *Proc. In Society for Information Technology & Teacher Education International Conference*. Las Vegas, NV, SITE'08: 1.

[15] Munson, S.A., Avrahami, D., Consolvo, S., Fogarty, J. Friedman, B., Smith I. 2012. Sunlight of Sunburn: A survey of attitudes toward online availability of US public records. *Information Polity*, 17(2), 99-114.

[16] Odom, W., Zimmerman, J., and Forlizzi, J. 2011. Teenagers and their virtual possessions: design opportunities and issues. *Proc. on Human Factors in Computing Systems*. Vancouver, BC, CHI'11, 1491-1500.

[17] Ofcom. 2012. Adults media use and attitudes report. Retrieved September 12, 2013. http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/

[18] Panteli, N., Marder, B., and Davenport, J. H. 2013. Through the lens of age; situated identities online across different generations. *Proc. British Academy of Management.* BAM'13.

[19] Patel, K. 2012. How do you brand consumer privacy – Internet giants take their cases to the masses with ad campaign. AdAge Digital, *Retrieved December, 18 2013*. http://adage.com/article/digital/brand-consumer-privacy/232694/

[20] Pew (a). 2013. *Teens, Social Media and Privacy.* Washington, DC: Pew Research Center's Internet & American Life Project.

[21] Pew (b). 2013. *Where Teens Seek Online Privacy Advice.* Washington, DC: Pew Research Center's Internet & American Life Project.

[22] Poole, E.S. and Peyton. T. 2013. Interaction design research with adolescents: Methodological challenges and best practices. *Proc. Interaction Design and Children*. New York, NY IDC'13, 211-217.

[23] Prensky, M. 2001. Digital Natives, Digital Immigrants. *On the Horizon, 9*(5).

[24] Saxby, S. & Knight, A. 2013. Identity crisis: Global challenges of identity protection in a networked world. In *Law & Practice: Critical analysis and legal reasoning*, S. Kierkegaard, Ed. International association of IT Lawyers, Copenhagen, DK, 13-29.

[25] Secure Identity Across Borders Linked, (Stork). *Retrieved August 26, 2013*. www.eid-stork.eu/

[26] Stevenage, S.V., Whitty, M. and Saxby, S. 2013. Who am I?: SuperIdentity. *International Innovation*, Research Media Inc. 82-84.

[27] SuperIdentity project. *Retrieved August 23, 2013*. www.superidentity.org

[28] Thomas, L. and Briggs, P. 2013. Teenagers' attitudes and design values around identity management. *Proc. on Human Factors in Computing Systems.* Paris, France, CHI'13.

[29] Toth, N., Little, L., Read, J.C., Guo, Y., Fitton, D., Horton, M. 2012. Teenagers talking about energy: using narrative methods to inform design. *Proc. on Human Factors in Computing Systems*. Austin, TX, CHI'12, 2171-2176.

[30] Voki Classroom. 2013. Oddcast Inc., New York. http://www.voki.com/

[31] Woelfer, J.P. 2012. The role of music in the lives of homeless young people in Seattle WA and Vancouver BC. *Proc. on Human Factors in Computing Systems*. Austin, TX, CHI'12, 955-958.

[32] Wright, D., Gutwirth, S., Friedwald, M., De Hert, P., Langheinrich, M., and Moscribroda, A. 2009. Privacy, Trust and policy-making: Challenges and responses. *Computer Law and Security Review 25*, 69-83.

[33] Yarosh, S., Radu, I., Hunter, S., & Rosenbaum, E. 2011. Examining values: An analysis of nine years of IDC research. *Proc. of the Conference on Interaction Design and Children*. Ann Arbor, MI, IDC '11, 136-144.

[34] Yoo, D., Huldtgren, A., Woelfer, J.P., Hendry, D.G., Friedman, B. 2013. A value sensitive action-reflection model: Evolving co-design space with stakeholder and designer prompts. *Proc. on Human Factors in Computing Systems.* Paris, France, CHI'13, 419-428.

[35] Zhao, X., Salehi, N., Naranjit, S., Alwaalan, S., Voida, S. Cosley, D. 2013. The many faces of Facebook: Experiencing social media as performance, exhibition and personal archive. *Proc. on Human Factors in Computing Systems.* Paris, France, CHI'13, 1-10.