


SUPERIDENTITY: Linking online and offline identities

Year 2 Progress Report

Sarah Stevenage
Sue Black
Sadie Creese
Richard Guest
Oriana Love
Steve Saxby
Danaë Stanton Fraser
Monica Whitty

Chris Bevan
James Doodson
Lia Emanuel
Hongmei He
Duncan Hodges
Alison Knight
Greg Neil
Bill Pike
Jean Scholtz

This report can be downloaded from:
http://www.southampton.ac.uk/superidentity/reports/index.page

October 2013

Table of Contents

1. The SuperIdentity Team

The Super-Identity project is an ambitious proposal covering a range of disciplines. This annual report outlines the knowledge and experience of the Investigators, and the progress made within Years 1 and 2 of the Project.

Anatomical and Behavioural Indicators of Identity: Offline World

Expertise is provided by Professor Sue Black (Dundee), Dr Richard Guest (Kent) and Dr Sarah Stevenage (Southampton). Together, they bring considerable experience in anatomical and biometric measures of identity in the real world environment.



Professor Black is the most experienced forensic anthropologist in the UK advising on issues of identification both at home and overseas. Dr Guest brings expertise in the field of automated biometric systems most notably in the areas of handwriting and dynamic signature verification, biometric image analysis, classification architectures and system interaction.

Finally Dr Stevenage acts as Principal Investigator for the project, and brings a cognitive psychology perspective on the human capacity to identify individuals from a range of static and dynamic cues in the real world including the face, voice, and gait. Together, these Investigators hold grants totalling nearly £5million from EPSRC, EU and other national and international funding bodies including government and industry. In addition, the Investigators provide representation to policy makers at the highest level including UK Government, Interpol, and International Standards (BSI and ISO).

Novel Behavioural Indicators of identity: Cyber World


Expertise is provided by Professor Monica Whitty (Leicester) and Professor Danaë Stanton Fraser (Bath). Professor Whitty's main area of expertise is cyberpsychology, with a focus on the capacity to self-present either truthfully or untruthfully through cyber behaviour. Recent work explores online relationships, internet infidelity, representation of self online, use of the internet by married couples, cyberstalking, Internet surveillance, deception across different mediums, engaging in symbolic taboo activities in video games, and online scams. She has been the PI on several grants notably on online surveillance and privacy; and deception across different modes of communication. Currently she is the PI on an ESRC funded project on the online romance scam. Monica also holds funds with Professor Creese (below) to explore aspects of Insider Trading.

Professor Stanton Fraser's area of expertise is human-computer interaction, with a focus on exploration of adults and young people's interactions with technology. She has been funded by numerous research council, business/industry and charity awards. She was CI on the EPSRC

'Cityware' project exploring trust relationships in the design of mobile and pervasive applications; and PI on the DTI/EPSRC 'Participate' project exploring pervasive computing for mass participation in environmental monitoring. Danaë currently holds collaborative funding to explore interdisciplinary aspects of Digital Identity.

Digital Security, Modelling and Data Visualisation

Expertise is provided by Professor Sadie Creese (Oxford) and Dr Bill Pike, Oriana Love and Jean Schultz (PNNL – US). Professor Creese is Professor of CyberSecurity at Oxford University, and is based in the Department of Computer Science. She is recipient of an IBM Faculty Award (2009) and is a member of various advisory groups with concerns spanning 'Global Uncertainties', the International Systems Security Association UK, and Cloud Security. She is PI on 3 collaborative projects funded by EPSRC and an additional grant with Professor Whitty on Insider Trading.

Dr Pike, Oriana Love and Jean Schultz are Senior Research Scientists in visual analytics, and research coordinator for the National Visualization and Analytics Center at PNNL. In conjunction with both government and industrial partners, they lead work on behavioural modelling of actors on a computer network for anomaly detection, the creation of temporal visualization techniques for pattern discovery in communications activity, interactive decision support capabilities for emergency management, and online visualization tools for the personalized display of social network data. Dr Pike has additionally served as Chair of the 2010 and 2011 IEEE Conferences on Visual Analytics Science and Technology.

Legal Representation

Expertise is provided by Professor Steve Saxby (Southampton). Professor Saxby is Director of the Institute for Law and the Web and is Professor of IT Law and Public Policy. He is co-founder of the International Association of IT Lawyers and the LSPI conference. He formerly served on the Legal Advisory Board of the European Commission, and the Intellectual Property Committee of the British Computer Society. He has been a Consultant to JISC; Ordnance Survey; Netherlands Council for Geographic Information; Countryside Agency, and Southampton City Council. Notable recent activities include the 2010 'WeGov' project (Where e-Government meets the e-Society) and legal consultation to the GeoData Insititute in their audit of data policy for the Crown Estate Office.

Contact Us:

By Mail:

SuperIdentity Principal Investigator:
Dr Sarah Stevenage
Psychology
University of Southampton
Highfield, Southampton,
Hampshire
SO17 1BJ

By Telephone:

SuperIdentity Administrator: Mrs Barbara Seiter
Tel: 02380 595578

By Email:

Superidentity@soton.ac.uk

Our Website:

www.superidentity.org
www.soton.ac.uk/superidentity

2. The SuperIdentity Project Brief

Our Context

In modern society, the risk associated with unreliable means of identification is felt in terms of a threat to personal privacy, information, intelligence, and resource. In the context of identity fraud, a recent assessment by the National Fraud Authority estimates the costs of UK identity fraud to exceed £2.7 billion per year, affecting 1.8 million people with much of this impact hitting the public purse. Allied to this, a government review commissioned in 2010 suggested that the capacity to obtain counterfeit identification documents contributed to the illegal entry into the UK of between 863,000 and 1.1million individuals, with a significant cost to national infrastructure and a potential threat to national security. Finally, failure to assure identification carries a cost in terms of criminal proceedings. Indeed, identification of the wrong suspect can contribute to the criminal trial, conviction and sentencing of an innocent party, together with a failure to pursue the true perpetrator. Technological enhancement means that identity can now be revealed, and counterfeited, in complex ways both in the physical and cyber world in a manner that existing models of identity and identification cannot keep up with. The SuperIdentity (SID) project represents an urgent and necessary response to this issue.

Our Aims

SID offers an innovative and exciting new approach to the concept of identity. The assumption underlying our hypothesis is that whilst there may be many dimensions to an identity – some more stable than others - all should ultimately reference back to a single core identity or a 'SuperIdentity'. The obvious consequence is that identification is improved by the combination of measures. SID takes this approach further than any existing work, and we achieve this by including static and behavioural measures from both the physical and the cyber world. Indeed, as perhaps the fastest growing identity domain, and the fastest changing means of self-representation, cyber-identity must not be ignored in models of identity.

SID provides two capabilities that are unique. First, we offer an identity framework through which associations can be made between different identity measures. The value of these associations is that one known piece of information may then be used to predict another previously unknown piece of information. This sort of approach is commonly used within e-commerce to enable analysts to predict that a shopper who purchased Product X might also be interested in Product Y. However, this approach has not been used previously in the realm of identity, and offers significant value to security and intelligence services. Second, we offer the capacity to quantify the certainty associated with an identification decision. This enables the end-user to have a level of confidence (or risk) in their decision, and to make a judgement as to whether additional information is required.

Our Objectives

Our aims are expressed through 3 objectives:

(i) to combine identity measures across real and cyber domains to inform identification decisions in the face of partial and changing knowledge and uncertainty;

(ii) to uncover hidden data and relationships between data which can contribute to informed decisions about identity; and

(iii) to quantify the certainty of an identification by quantifying the reliability of each contributing measure.

3. Executive Summary

Our work has been united by a common goal – to understand how the various aspects of identity relate to one another and combine to reflect who we are. Our interest is partly theoretical – with a deep motive to understanding how digital living may influence how we represent ourselves. Additionally, our impact and applied value comes through support to investigative and legal process by assisting identity and identification decisions across physical and digital contexts.

Biometrics

Within the physical context, our analysis of biometrics has highlighted the accuracy and confidence with which identity can be determined from cues in isolation and in combination. Parallel strands of work compare the performance of the human and the automated system, and this comparison enables us to determine which source will be more reliable under circumstances that range from optimal to impoverished. For example, when recognising a face, the human perceiver can relatively easily overcome changes to pose or expression whilst the automated system cannot. Similarly, when processing an iris scan, humans and machines make different errors, and optimal performance is demonstrated when human and machine decisions are combined.

More exciting within this field has been the investigation of novel biometric cues. Hand geometry, and hand vein analysis, have proven themselves as valuable cues to identity, and our research now provides evidence that has gained academic peer review, and admissibility into UK court contributing to a number of convictions.

Cybermetrics

Within the digital context, our study of cybermetrics – cyber cues to identity – has revealed a number of measures which reliably indicate aspects of identity. For example, our fingerswipe on a mobile device can leak our likely age, sex, handedness, and digit length and the latter may, of course, indicate height, stride patterns and other related biometric characteristics. Similarly, through the collection of a unique database of information – the SuperIdentity Stimulus Database (SSD), we are exploring other cybermetrics including our keystroke dynamics, facebook profiles, privacy settings, and social networks. These metrics start also to interface with the more choice-based cybermetrics that interest us. Our work reveals that our online profiles differ depending on the cyber context, highlighting different aspects of our selves according to the norms of the site. Similarly, our work reveals different patterns of lying and truth-telling across contexts. Individuals tend to lie most in face to face interactions, but the next most common ways to tell a planned lie are via phone or text – both being lean modes of communication. This tells us where we are most likely to be able to trust information in different digital contexts.

In another innovative line of work, our project sheds light on how personality and experience can shape the icons or avatars that we create online, and the levels of privacy and risk with which people use passwords. Each of these is important if we are to fully understand online identity. Most of the time, these cybermetrics will indicate that an online identity links with a single individual in the real world. However it is equally possible that our cybermetrics will reveal such a chaotic pattern that there is no other conclusion than to believe a range of individuals share a single online identity.

Social Acceptability and Legal Privacy

In introducing themes of risk and privacy, our project has also provided a focus on issues of

social acceptability, privacy, trust, and the right to be forgotten. Through a series of workshops with a group of high volume internet users, we reveal how individuals use different online social spaces for different purposes, and we explore the norms of interaction within those social spaces. Participants have explored the judgements they make about one another based on an avatar, and have considered the information that they are happy to reveal as well as the information they want to maintain private. The latter category includes metrics such as fingerprints, true date of birth, location and address, and yet metrics such as usernames and passwords may be less well protected because of a view that they are 'disposable' or changeable.

The legal reforms within the UK, EU and US have also shaped our consideration of identity protection and identity management. The EU's debated data protection regime provides greater privacy rights to individuals, and this is accompanied by the imminent introduction of an Identity Assurance Service to minimise identity fraud at a time when almost 1 in 5 people have had their online accounts hacked and have suffered financial losses.

Against this context, one of the most exciting strands of work completed to date involves the use of our SuperIdentity framework as a source of feedback on how much people actually reveal about themselves online. Within the context of a 'privacy by education' initiative, the impetus to raise awareness to safe digital living sits behind our recent application to the Royal Society Summer Science Exhibition 2014.

Modelling and Visualisation

Our uniquely powerful SuperIdentity framework has been developed by colleagues at Oxford and combines the weight of theoretical and empirical evidence examining bio and cyber metrics of identity. This framework models identity and identification under situations of uncertainty by combining each piece of identity evidence. Not only can we then predict likely identity, but we can also index that prediction with a level of confidence, and can indicate what additional information could be provided to make that identification more reliable. We are now at a stage in our development where the SuperIdentity model can combine known information to predict identity, reveal previously unknown information based on demonstrable correlations between identity cues, demonstrate how identification can be enhanced, provide confidence estimates, and can correct false assumptions when two individuals may be masquerading behind one persona.

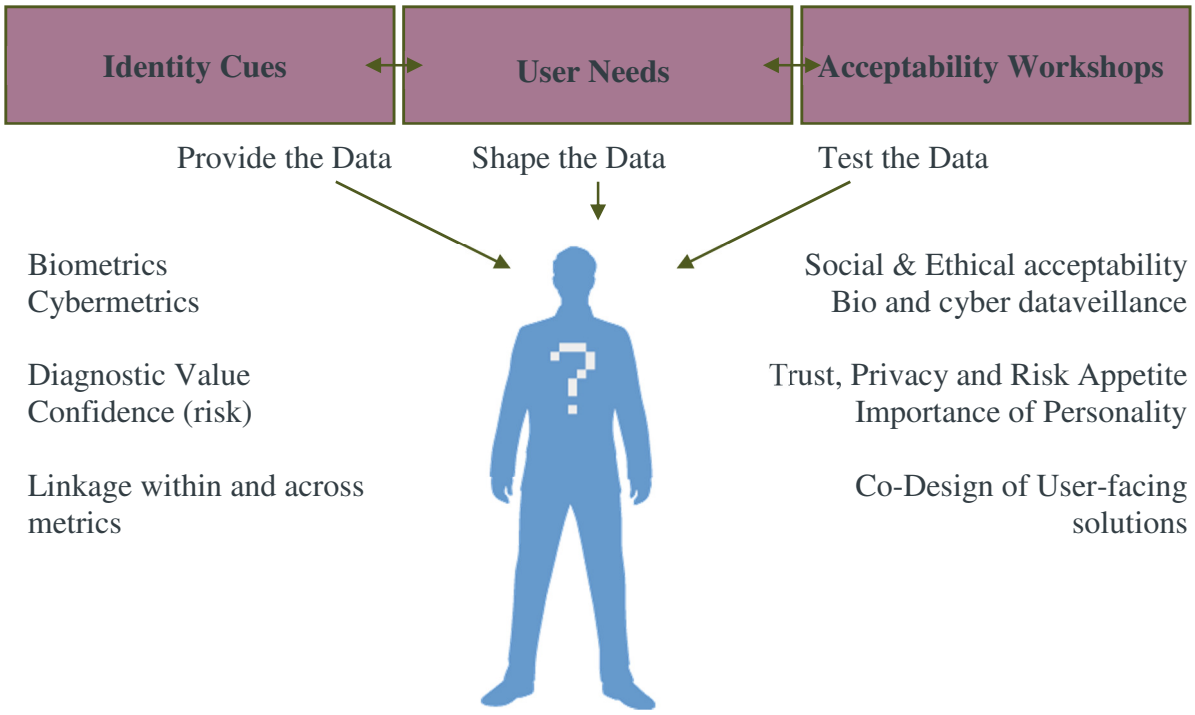
This framework is transformed into a usable interface through the latest visualisation techniques, guided by a survey of use-cases provided by UK and US analysts who make identity decisions as part of their day-to-day roles. Through participatory workshops, users act as design partners to refine our visualisation tools towards a usable and powerful tool.

And now…

Looking forwards, the SuperIdentity project now tackles one of our most exciting challenges – the capacity to link physical and digital identities. Several measures present themselves as potential bridges between the physical and digital domain. For example, the cybermetric of a fingerswipe might readily reveal biometric cues related to the hand and the physical frame of an individual. Similarly, the avatar that an individual chooses may reflect aspects of actual physical appearance such that reverse-engineering to create a physical likeness may be possible. This, undoubtedly, will be mediated by a host of cues, not least of which is the personality of the individual. These, however, are measurable mediators, and exploration in this domain represents an innovative and exciting next step.

4. The SuperIdentity Methodology

Within Year 1 of our project, we defined our approach as drawing on three critical sources of information:



Within Year 2, we have made substantial progress in each of these areas, and the sections that follow outline our major findings. Here, we provide the rationale for our approach and for their combination.

Identity Cues

Where the SuperIdentity project extends beyond existing work is in the exploration of identity cues across both the physical world and the cyber world. In the physical world, we refer to biometrics, and recognise the work on a dominant set of established biometrics such as fingerprints, gait, iris scans, and face. Our approach has been to use a single set of stimuli as a basis to test the accuracy of identification decisions made (i) by humans and (ii) by the best of the available automated systems. By using the same set of stimuli, we have the capacity to draw a direct comparison between human and automated strengths and weaknesses.
In addition to these very traditional biometrics, we have also examined more novel biometrics including the voice, and the hand (geometric and vein patterns). Our work on voice recognition has helped to define the conditions under which it can be considered valid. Alongside this, our pioneering work on hand vein analysis in particular means that this novel biometric now has evidential admissibility and academic acceptability through peer review.

In the digital world, we refer to cybermetrics. However, whilst our work recognises the identification value of static cybermetrics such as usernames or passwords, the SuperIdentity team has taken the view of cybermetrics further by recognising more dynamic cybermetrics reflecting behaviours or choices. These include attitudes, choices, and behaviours surrounding password risk, identity management across different online spaces, and the disclosure (or otherwise) of secrets or planned lies across different modes of communication. The latter two lines of enquiry are of particular interest because our approaches enable us to examine behaviour across both physical and digital environments. This supports a critical aspect of the

SuperIdentity project which is the capacity to explore the extent to which identity, and identity management may be linked across the physical and the cyber worlds.

The SSD

The biometric and cybermetric work described above is supported through the generation of a completely novel and exhaustive database – the SuperIdentity Stimulus Database (SSD). Within Year 2 of our project, considerable effort was put into the construction of this database in which 121 individuals have provided all known cues to identity that we could imagine. These included biographical information, biometric cues (both static and behavioural), cybermetric cues (both static and behavioural), and a battery of personality measures. A total of 116 individuals have given consent for their data to be released as part of a licenced database for research purposes.

What is unique about this database is the breadth of measures recorded, making it possible to explore the accuracy of identification from each measure. More interestingly, this database enables the SuperIdentity team to see where potential exists to link physical and cyber identities together. Focussed and statistically powerful enquiries can then be directed to further these promising avenues, and this represents the work of Year 3.

Neil G.J., et al. (final draft) The Southampton Stimulus Database: Physical, digital and psychological measures of identity.

http://www.southampton.ac.uk/superidentity/ssd/ssdhomepage.page

Welcome to the SuperIdentity Stimulus Database Website!

User Needs

Our user-cohort has been recruited from amongst a group of professionals who identify individuals, or gather evidence, as part of their day-to-day roles. In the US, these individuals span the fields of Law Enforcement, Intelligence analysis, Border Control, Consumer Research, Fraud, and Corporate Security. In the UK, these individuals span various government agencies and commercial companies. None are named here.

The purpose of the User Cohort is to direct the functional requirements of the eventual SuperIdentity framework. Through semi-structured interviews, their insights into the desired capability of a SuperIdentity system have helped to inform both the data to be gathered in the SuperIdentity Stimulus Database; and the flexibility and customisation of the SuperIdentity model itself. The outcomes of these interviews are summarised later in this document.

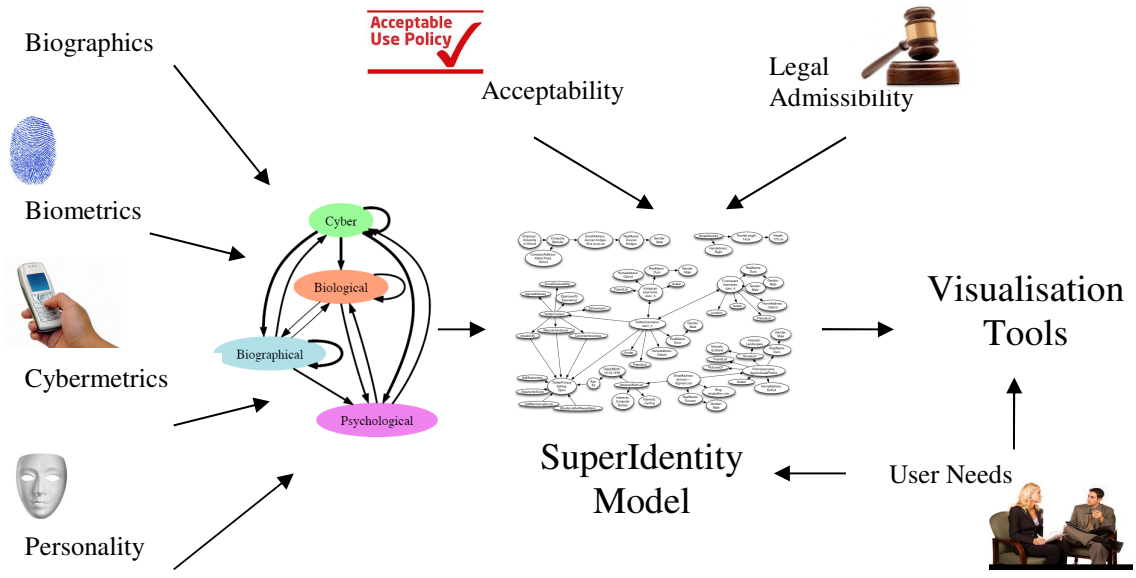
Acceptability Workshops

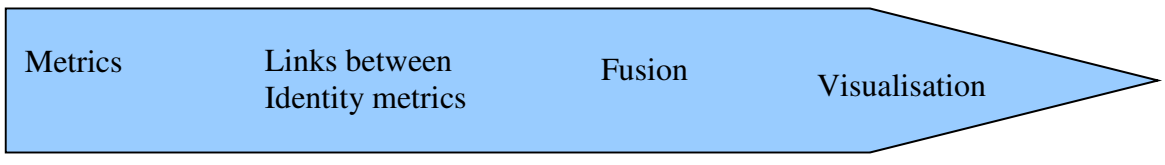
The participant cohort represents a special group of participants who will follow our project across a two year period. They will be recruited to take part in experimental studies, and this will enable us to address the possibility of 'generic-recognisers' who are notable at recognising individuals within and across metrics.

However, the real value of our participant cohort is in their role in providing a social reflection on the acceptability of a SuperIdentity framework, and the levels of education or risk-taking that individuals show to their (super)identity information. The team at Bath have specific expertise in working with participant cohorts, and they bring this to bear in the recruitment, engagement, and involvement of a group of 13-18 year olds. This cohort represents an under-researched group of nevertheless high-traffic online users. Consequently, such a cohort provides the team with a very rich opportunity to learn about the ethical and social acceptability issues concerned within a modern identity context.

Combination of Information

All sources of identity information, once tested or established through the literature, feed the articulation of identity links through our SuperIdentity model. Social acceptability, and legal and ethical consideration shapes our understanding of response to this combinatorial approach, and user needs shapes both its value and its visualisation in support of a fuller understanding of identity and identification processes.





5a. Current Findings: SuperIdentity Use Cases

The SuperIdentity project has been grounded by our very early engagement with individuals who, through their jobs, have a need to make identity or identification decisions. As such, colleagues at the University of Bath, Oxford, and Pacific Northwest National Laboratory (US) have driven forward a significant initiative to gain an understanding of the user perspective.

In total, interviews were conducted with 8 intelligence analysts, 8 law enforcement officers, 1 missing persons analyst, and 1 director of cybersecurity within UK banking. Whilst the emergent themes amongst US users were broadly echoed within the UK, there were some important differences noted, particularly in terms of the awareness that a single user may have of the whole picture. The aim with this piece of work was to inform the SuperIdentity model so that we understand and prioritise the most relevant measures, and the most likely links between measures to support identification.

Through semi-structured interviews, designed to be unclassified, broad themes emerged. First, it was noted by our users that not everyone under their scrutiny is suspected of being a 'bad guy'. In this sense, identification was seen as one of a larger set of goals that the users may have. Second, the issue of online deception was flagged as important. The capacity to build confidence in identification was seen as desirable, through building constellations of corroborating evidence as a potential way to overcome online deception. Third, the issue of provenance was noted – a sense of knowing the source and thus the likely accuracy or reliability of information.

Each user also identified a series of other more tailored priorities that provided valuable context for the SuperIdentity project. For instance, in an intelligence or law enforcement context (i.e., investigation of foreign interests, investigation of immediate threat), there will often be a particular need for real-time information, whereas in a more corporate setting (i.e., investigation to confirm and profile company involvement) the onus is more often on consistency of information across sources rather than on the speed of obtaining that information. At the level of intelligence gathering, priorities may lie in profiling an individual and identifying real names, known associates, or potential affiliations where information may be sparse or deceptive, and this will have greater or lesser urgency depending on the reason of interest (i.e., cyber-attack). Equally, the intelligence arena has a need to determine the reliability of source information so that the provenance of any intelligence can be verified.

As an output from these interviews, two canonical Use Cases were identified. The target use cases are inspired by actual use cases collected from the law enforcement, intelligence and industry. These use cases showcase the need for the SuperIdentity model's ability to transition through the Biographical, Biological, Psychological and Cyber domains. The use cases were crafted to highlight the potential appeal to our stakeholder and steering committee, appeal to the public and have coverage across the different domain areas. At the end of the SuperIdentity project in late 2014, we plan to have enough supportive research to demonstrate how the identity model helps solve these cases.

Canonical Use Case 1: From Username to the Person

> Given an individual's username, determine who that person may be in the physical world in terms of their real name, skills, age, beliefs, etc. Actionable intelligence may be obtained even if the real name cannot be derived with confidence. Target audience: Intelligence, law enforcement.

Description

A suspicious article was posted online that gets attention of the intelligence community. The IP address was tracked to an internet café in a large city. At this café, several incomplete data points were collected: low-quality surveillance video from the past two weeks, hundreds of fingerprints, and some credit card information. In addition, the username of this individual, the text written, the blogging site where this information was posted and several user comments were collected. The host of the blogging site was not able to share any additional information. The investigator wishes to understand who this person is (and quickly). In particular, they would like to know the identity of the user, if the account is shared or individually owned, the associates of this person, their skill level, age, gender, and ideology.

* Note: a slight variation of this scenario that has occurred with law enforcement historically first appears as a hand-written note to newspapers/ government employees.

Domains

Cyber (username, writing samples- look at this over a period of time, account sharing)
Biographical (location, associates, real name, expertise, age, gender, credit card into)
Psychological (ideology- look at this over a period of time)
Biological (fingerprint, gait, face)

Implications for the SuperIdentity tool

Annotate publicly vs. privately available data; white list vs. black list
Sort according to the amount of trust in data…
Select/deselect data sources types (open source, confidential, etc)
Show confidence of each link between one piece of information and another
Provide a mechanism for users to increase confidence of a element's value
Re-route options. Critical path analysis, i.e. show that element C is necessary to continue.
Allow users to update and confirm confidence
Allow users to start anywhere in the path—don't presume they need to navigate the entire tree.

Inspired by actual use cases

Use Case #10 Cyber attack preparation and hacker profiling [Intelligence community]
Use Case #6: Anonymous user handle

Canonical Use Case 2: Identifying an Individual within a Crowd

> During a public protest, law enforcement is monitoring the crowd to ensure all is peaceful. A subset of the protesters belongs to a vocal social network that has resorted to violence in the past. Law enforcement wants to most closely monitor those online ring leaders in the crowd.

Description

A public protest has just begun unexpectedly at a well-known area of downtown. Law enforcement is working to identify the individuals of interest within a crowd in an effort to mitigate any issues, but only know about this group's views and leadership based on their vocal and unsettling online presence in discussion forums. Low quality video surveillance is being leveraged to help with monitoring and is doing a good job capturing the features of most participants within the crowd. The law enforcement challenge is to understand how the participants within the crowd map to the actors within the group's online discussion forum.

Domains

Biometric (gait, height, facial features, observable features)
Cyber (discussion groups, social friend/follower network analysis)
Psychological (ideology)
Biographical (arrest record, real name)

Implications for the SuperIdentity tool

Real time information is paramount in this use case, so a "sort by automatable" feature would be of interest.
Several individuals (rather than just one individual) might be investigated at once.
Eliminating an individual (rather than attributing an individual) is also a valid conclusion.

Inspired by actual use cases

Use Case #12: Deceptive, organized vandalism
Use Case #13: Homicide
Use Case #17: Property Crime
Use Case #5: Organizational Informant

5b. Current Findings: Biometrics

Within the Superidentity team, we recognise that cues to identity exist in the physical world and in the digital world. The physical cues we term 'biometrics' and these are explored by colleagues at the Universities of Dundee, Kent and Southampton. Progress is summarised here in terms of our understanding of the value of our biometric cues. We gratefully acknowledge our collaboration with the CAST unit within the Home Office during Year 2, and we look forward to a fruitful collaboration with the Metropolitan Police during Year 3.

Traditional Cues:

The Face

So far, our empirical work explored the capacity of man and machine to perform during a series of biometric recognition tasks. In terms of automated face recognition, we have devised a methodology to assess the relative performance of facial recognition systems with respect to the following characteristics: system performance (in terms of correct identification rate), number of subjects in a watch-list, environmental considerations and distance to camera. This framework can be used to inform the expected system performance of a combination of factors given previously calculated error rates.

> He, H., & Guest, R.M. (2013). A Configurable Multi-Engine System Based on Performance Matrices for Face Recognition". IEEE: HST conference, Boston, November 12-14th 2013

Similarly, human face recognition performance has been assessed both through reference to the extensive published literature, and through novel empirical testing, with the aim of informing the project of the conditions under which human recognition will be most optical. In this regard, our results support the literature in emphasizing the importance of a ¾ viewpoint even in rich conditions involving video-based information.

Full face **Mixed** **¾ Profile**

(i) Metacognition:

Our use of cognitive psychological techniques enabled us to explore not only how well an individual performed on a recognition task, but how well they believed that they performed.

This becomes important in the absence of ground truth. In such a situation, how do we know if an identification is right?

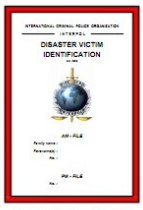
This analysis of metacognitive monitoring led us to highlight the validity of a report/withhold decision in that participants were usually correct when they felt sure enough to report their decisions to an authority figure. Moreover, the report/withhold decision is attractive as a measure because its categorical nature avoids the inherent problems when simply measuring confidence in that people differ in their overall levels of confidence and in their use of a scale to reveal shifts in their confidence.

Stevenage, S.V., & Neil, G.J. (2012). Knowing What you Know: Using Metamemory to Predict Accuracy of Eyewitness Identifications. *IA-IP*. 5-7 December, London.

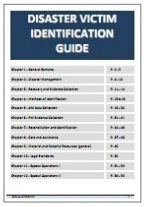
(ii) Objective Descriptions:

AM Forms (yellow)

PM Forms (Pink)



Reconciliation Report



DVI Guide

Across the course of our work, we have also been able to compare human and machine analyses of the same facial stimuli in order to determine whether one may be a better source for some information. In this regard, we used an objective method of facial description based on the Interpol Disaster Victim Identification Ante-Mortem forms. The Interpol AnteMortem form provides a thorough, accepted, and objective set of descriptors through which to capture facial characteristics.

This may overcome what has become known as the 'semantic gap' – the distinction between what people see and what they can linguistically convey. With this in mind, we have completed the data collection phase of a substantial survey in which 116 faces have been described both by human perceivers, and by automated Interpol feature extraction. Our objective is to determine the level of agreement amongst human perceivers (are the Interpol descriptors consistently used?) and the level of concordance between the human and the machine. If high levels of agreement are revealed, the Interpol form may provide a valuable and objective tool to assist in facial description of a person of interest.

(iii) Expertise (Super recognisers):


Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Femail | Health | Science | Money | RightMinds

News Home | Arts | Headlines | Pictures | Most read | News Board

The man who NEVER forgets the face: How Scotland Yard's elite squad of 200 'super recognisers' can spot a suspect in a crowd

Within the Metropolitan Police, there is a group of officers known as super-recognisers through their remarkable ability to recognise individuals. The opportunity to contrast their performance with that of our control participants will enable us to speak to the issue of the markers that may make a spectator more trustworthy as a source of information. A series of studies are anticipated which explore whether their notable face recognition skills generalise to support good voice recognition, or may be reflected in more effective metacognitive monitoring, suggesting that these individuals better *know* when they are right, and when they are wrong.

The Voice

Our own work within the Superidentity project supports the published literature in suggesting that voice recognition is generally not as accurate or robust as face recognition. Whilst familiarity assists in the recognition of an individual from their voice, familiar voice recognition still lags behind familiar face recognition. In contrast,

when unfamiliar, voice recognition achieves better than chance levels but shows only a 63% hit rate and a 39% false alarm rate. In the same recognition task, unfamiliar face recognition achieves a 93% hit rate and an 8% false alarm rate.

Within the Superidentity project, we were also keen to understand how recognition performance might be affected by contextual factors. As such we tested voice recognition when faces were present, when face and voice identities conflicted to create ambiguity, and when distraction was provided.

(i) Facial overshadowing

Our results showed that performance in voice recognition was substantially impaired when a face is presented at the same time. This is known as facial overshadowing. In fact, performance levels for unfamiliar voice recognition fall to no better than chance overall, (59% hit rate, and a 49% false alarm rate) when the face is simultaneously presented whilst face recognition is untouched by the simultaneous presentation of a voice (92% hit rate, 11% false alarm rate). These results provide an important window into the moderating effect of context on the value of a biometric. When unfamiliar voice recognition is under scrutiny, users may be wise to not rely on performance if a face was visible at the same time.

(ii) Conflict

We also explored what happened with familiar stimuli when faces and voice were presented simultaneously. In this experiment, the faces and voices of celebrities were paired so their identities either matched or did not match. In matching conditions, face and voice recognition was good – each cue helped recognition of the other. However, in mismatching conditions, face recognition remained good but voice recognition was overridden by the presentation of another celebrity's face – again facial overshadowing was evident but this time with highly familiar individuals.

> Stevenage, Sarah V., Neil, Gregory James and Hamlin, Iain (in press) When the face fits: recognition of celebrities from matching and mismatching faces and voices. Memory.

(iii) Distraction

Interlopers are those stimuli that may be presented between study and test, or between witnessing a crime and providing a statement or a line-up recognition. Across a series of tests, our results suggest that interlopers have a significant effect on the recognition of an unfamiliar voice. Moreover, the impairment in performance occurs regardless of how many interlopers are experienced, and of how similar those interlopers are to the target voice.

One aspect of good news is that some voices are more protected against interlopers than others. Again, our tests show that unfamiliar voices that are naturally distinctive, or that have been repeatedly experiences (heard 5 times) receive less impairment than those that are naturally typical or have been heard only once.

> Stevenage, Sarah V., Neil , Greg J., Barlow, Jess, Dyson, Amy, Eaton-Brown, Catherine and Parsons, Beth (2012) The effect of distraction on face and voice recognition. Psychological Research, 77, (2), 167-175. (doi:10.1007/s00426-012-0450-z).

(iv) Face-voice matching

Finally, our work has explored the extent to which we may be able to pair an unfamiliar voice with its face. In line with recently published evidence, our data suggest that performance is

better than chance on this task but is still not high. One possibility is that when we use scripted speech in experimental tasks, we lose some natural vocal characteristics and thus minimise the potential for higher levels of performance. Work is currently underway to test this possibility.

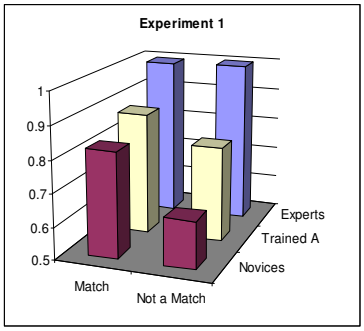
The Fingerprint

(i) Expert methods

Through qualitative methods, we explored the approach taken by 14 Fingerprint Experts at Netley Fingerprint Bureau, Hampshire. Our question was the extent to which these experts adhered to a common methodological approach. This enquiry gains significance in light of the Shirley McKee case in which fingerprint evidence was questioned within the court setting.

Our results suggested that the methodology used by fingerprint experts within this bureau clearly met the strict Daubert standards of admissibility as used by the US court system. Experts described an ACE-V method, consisting of Assessment of the finger mark from the crime scene, Comparison with the controlled set of prints under consideration, Evaluation, and finally, Validation by a second expert. Our participants took their time and showed consistency in their approach with no variation related to the number of years in service.

(ii) Fingerprint Training



The verbal protocol provided by our experts above enabled the development of a training tool for novices. In this regard, our aim was to see whether this training tool would be clear enough to explain to a lay person such that their level of fingerprint analysis may approach that of the expert themselves.

Our results suggested that the training tool enabled significant improvement in the capacity to scrutinise matching and non-matching fingerprint pairs, and elevated performance above the level of an untrained novice. However, the experts were still significantly better than our trained novices and this may reveal the importance of the 'reality of an ecologically valid situation', or the unspoken (or unconscious) heuristics that an expert may bring to the task.

The Iris

The iris is rising in usage, and in acceptability as a biometric cue for authentication and identification processes. However, the literature has concentrated on automated iris processing techniques, and very little work has explored the capacity of the human perceiver in an iris matching task. We investigated the performance of human verification of iris images and compare against a standard computer-based method. Our results suggest that performance using a computer-based system is no better than performance of the human participants. Additionally and importantly, performance can be improved through incorporation of the human as a 'second decision maker'. This fusion system yields a false acceptance rate of just 9% when disagreements are resolved in line with strengths of each 'decision-maker'.

Guest, R.M., Stevenage, S.V., He, H., & Neil, G.J. (2013). An Assessment of the Human Performance of Iris Identification" IEEE: HST conference, Boston, November 12-14th 2013.

Novel Cues:

The Hand

(i) Geometry

At a systemic level, the literature suggests some evidence that hand geometry may usefully be used to glean some additional identity cues about an individual. The strongest line of evidence in this regard is the linkage between 2:4 ratio (index:ring finger) and the level of testosterone in an individual. Plausibly then, a high 2:4 ratio may be linked to other biometric characteristics indicative of sex including height, stride length, facial characteristics of jaw and brow, and fundamental frequency of voice. The Superidentity Stimulus Database allows us to explore these links across a set of 116 individuals. More interesting, hand geometry may plausibly be related to observable and measurable hand behaviours such as fingerswipes on a mobile phone, or pen-and-ink and finger signatures within physical and digital contexts respectively.

(ii) Canonicality or 'Viewpoint'

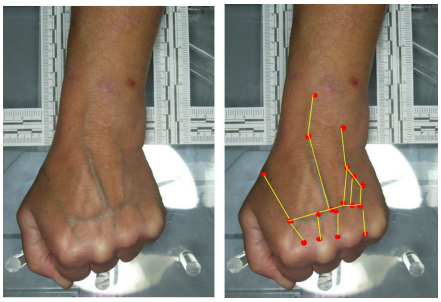


In collaboration with Dundee, the work at Southampton has explored the conditions under which hand recognition may remain robust. In particular, we have explored the impact of viewpoint in providing a canonical (ideal) or non-canonical (compromised) viewpoint of the hand for recognition purposes.

Our data in this regard suggest that hand recognition significantly declines but remains above chance levels even when viewpoint is non-optimal. Consequently the capacity to match a hand image from crime scene footage to suspect image, is possible and shows some resilience to a manipulation that can impair performance with other biometrics. Collaborative work between Southampton and Dundee continues in this field.

(iii) Hand Vein Analysis

The work of colleagues in Dundee has pioneered the acceptability of hand vein analysis within the court system, and within the academic peer review system. Through analysis of vein patterns, or motifs, it is possible to highlight the frequency of particular motifs across a group of individuals, and consequently, the distinctiveness of particular motifs within an individual. This analysis has helped to support a number of convictions within the UK court system, establish a reputation through caselaw for this novel biometric.



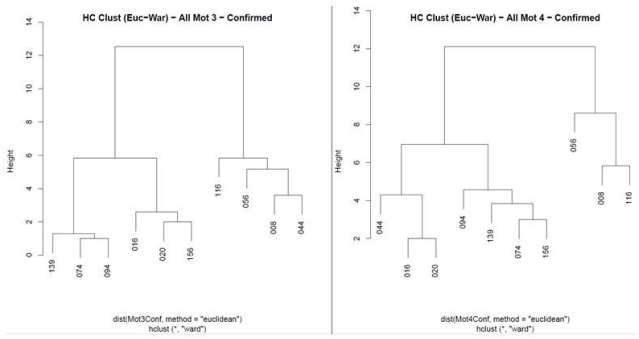


Figure 2 Example of cluster analysis dendrogram from preliminary analysis.

Black, S.M., MacDonald-McMillan, B. & Mallett, X. (2013). The incidence of scarring on the dorsum of the hand. Int J Led Med DOI: 10.1007/s00414-013-0834-7.

Black, S., MacDonald-McMillan, Mallett, X., Rynn, C. & Jackson, G. (2013). The incidence and position of melanocytic nevi for the purposes of forensic image comparison. Int J Leg Med. DOI: 10.1007/s00414-013-0821-z

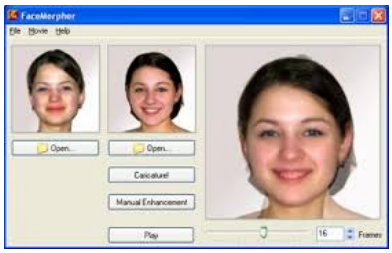
Jackson, G. & Black, S. (2013). Use of data to inform expert evaluative opinion in the comparison of hand images – the importance of scars. Int J Leg Med. DOI: 10.1007/s00414-013-0828-5.

Links to Cybermetrics

(i) Faces and Avatars

Experimental methods have been used to explore the issue of whether an avatar may physically resemble its creator with any degree of reliability. A new methodology for user-avatar similarity measurement was trialled here. The participants' self ratings of similarity correlated well with judges' ratings of similarity, and both correlated well with a more objective index of similarity based on the concordance of Interpol descriptors. Participants generating humanoid avatars unsurprisingly had greater similarity to their avatar than those who generated fantasy avatars. In addition, whilst personality had some minor influence on the likelihood to generate a humanoid avatar, a more useful determinant of user-avatar similarity was the physical attractiveness of the participant to begin with.

(ii) Reverse-engineering appearance



Discussion is now in hand to explore the utility of computer morphing techniques to generate a likeness of an individual based on their avatar and some indicator of physical attractiveness. In parallel with more established computer enhancement techniques, i.e., to age the appearance of a missing child, this work may support the generation of a likeness to bridge the physical and digital contexts and to assist with more robust routes for identification.

(iii) Hands, Finger-signing and Finger-swipes

Based on the data collected within the SSD, work is now underway through collaboration between the Universities of Bath and Kent, to establish whether any reliable linkage exists between an individual's physical hand geometry, and their observable hand behaviour through fingerswipes on a mobile phone, or finger-signatures on a device. Already in this vein, work has been completed examining the similarity between a pen and ink signature and a finger signature. A large number of features commonly used for physical signature assessment are related to input by swipe, albeit at a scaled value, suggesting commonality in the donation behaviours.

Robertson, J., & Guest, R.M. (2013). A feature based comparison of stylus and finger based signature characteristics. In: Proc: IGS 2013, Nara, Japan, June 2013.

(iv) Links between biometric cues and personality

The SSD also provides us the capacity to explore possibly links between biometric cues and personality indices. In this way, rather than there being measurable links directly between biometric and cybermetic cues, we may find that the association between the two is mediated by personality. The SSD enables us to explore links between one biometric and another, and between each biometric and a host of personality variables, and this speculative analysis will then guide more detailed experimental enquiry.

5c. Current Findings: Cybermetrics





Representation of Identity in online spaces gives rise to what we term 'cybermetrics' – those measures that can reveal identity in a digital space. The teams at Bath, Southampton and Leicester have been involved in a number of investigations within this domain.

Smart Phone Gestures

To a large extent, the gesture-driven touch-sensitive interactive screen has removed the need for physical buttons to interact with mobile phones. As highly sensitive instruments, touchscreens are able to provide researchers with access to more nuanced data about user interactions than could be obtained from two-state physical buttons and keypads.

Ongoing work by the team at Bath has explored the use of multiple 'swipe' gestures for the purposes of identification. Gestures were captured during user-interactions in four directions from a wide range of mobile smartphone users. Using four simple feature extractions *gesture length, completion time, touch pressure* and *gesture thickness* we were able to distinguish users by their gender, age range and by the hand used to create the swipes. By using cluster analysis techniques, we were further able to classify swipes into three distinguishable 'styles', based on contributions from all four feature extractions described. Finally, by examining how consistently each user created swipes within these styles, we found that all of our participants naturally created their swipes using no more than two of these styles. These findings are explored in terms of their potential utility for passive user verification and user identification via swipe gesture characteristics.

Twenty Statements Test: Comparing fictitious online and offline identities

Several of our teams have been involved in the exploration of identity across offline and online contexts. The question here has been 'how do people represent themselves in different settings?'

We have used the Twenty Statements Test to probe this question. It allows individuals to describe themselves in twenty statements, and we then ask whether they are happy to reveal their answers or whether they want to withhold or replace anything they have said. Our results demonstrate that people represent themselves very similarly across an offline and an anonymous online context. The latter may provide a sense of safety so that, despite having information visible in an online setting, individuals do not know who is looking at it so they feel no need to regulate their image. In contrast, when individuals represent themselves intentionally in specific online spaces, such as a dating site, or a professional site, then they tend to express aspects of their self that may be 'ideal' for that context.

Together, these data suggest subtle differences in how identity is managed in offline and online contexts: Changes in socially accepted norms across these contexts may guide individuals to display different aspects of themselves across these different spaces and this raises the interesting idea of a 'distributed identity'.

Twenty Statements Test: Comparing online and offline identities

Whereas the Bath and Southampton teams explored ficitious offline and online representations of identity, the team at Leicester provided a parallel exploration of actual representations across different online spaces (including online dating sites, LinkedIn and Facebook). These were compared these with individuals' perceptions of their overall self-concept. Rather than ask individuals how they believe they would hypothetically represent themselves in these spaces we were interested in individuals who actually used these sites and how they actually presented themselves on these sites.

Individuals were asked to fill in 10 statements describing who they were in everyday life as well as who they were on one of these spaces. We found that the self-concept differed to the self presented on different online profiles; however, these differences were not as pronounced as theorists would predict. We also found that individuals appeared to impression manage across different types of online sites. Interestingly, there was more consistency between the overall self-concept and Facebook self compared with the other two online spaces. Convergent with the work described above, we concluded here that the Internet affords different opportunities to present different aspects of identity. A paper summarising our findings is currently out for review, and the work has been presented at the Oxford Cybersecurity seminar series and as a keynote talk.

Whitty, M.T., Bevan, C., Emanuel, L.L., Neil, G.J., Jamison-Powell, S., Stanton Fraser, D., & Stevenage, S.V. (under review). Who am I? Self-concept across Facebook, dating sites and LinkedIn.

Whitty, M. (2013, April). Who am I: Identity across different cyberspaces. *Cyber Security Seminars: University of Oxford, April 25, 2013.*

Whitty, M. (2013, September). Keynote address: Who am I? Is identity consistent across physical and cyber spaces? *The First Annual Cyberpsychology Conference, De Montfort University, Leicester, September, 19, 2013.*

Big 5: Comparing online and offline identities

In Year 2 colleagues at Leicester completed data collection for the Big 5 study, which examined overall personality (as measured by the Big 5) and personality presented in four online spaces (Facebook, LinkedIn, Twitter, Online Dating). Again, we believed that it was important to examine real data rather than hypothetical situations. Preliminary findings suggest that individuals are more likely to under-represent themselves on consciousness and neuroticism on online sites, and over-represent themselves on extraversion and openness. In this study we also examined whether individuals who were high self-monitors were less likely to have disparity between selves; however, early findings suggest the opposite to be true. It appears that people high on self monitoring were more likely to have significant differences between their overall personality and personality represented on the various online sites (perhaps this is because of they are more savvy about the affordances of these spaces).

In line with previous research, our preliminary findings suggest that individuals who have greater disparity between their 'actual selves' and 'ideal selves' scored lower on psychological well-being. Preliminary findings have been presented at the Oxford Cybersecurity seminar series and as a keynote:

Whitty, M. (2013, April). Who am I: Identity across different cyberspaces. *Cyber Security Seminars: University of Oxford, April 25, 2013.*

Whitty, M. (2013, September). Keynote address: Who am I? Is identity consistent across physical and cyber spaces? *The First Annual Cyberpsychology Conference, De Montfort University, Leicester, September, 19, 2013.*

Risky password choices

In Year 2, together with the University of Oxford researchers, colleagues at Leicester completed the first of four studies, which investigated what types of people are more likely to select insecure passwords. In the first study we also examined experts' and non-experts' understandings of security risks (both online and offline). Our findings revealed that non-experts still require security education with regards to patching and updating software. In addition, experts were more likely to select secure passwords. Findings from this study were presented in the following paper and posters:

We have recently completed collecting data for the second study on password choice which again considers the differences between experts and non-experts passwords as well as whether personality (locus of control, Machiavellianism, Impulsivity and self-monitoring) has any influence on risky password choice. These data are yet to be analysed.

Creese, S., Hodges, D., Jamison-Powell, S., & Whitty, M. (2013). Relationships between password choices, perceptions of risk and security expertise. *HCI International 2013: Las Vegas, Nevada, USA, July 21-26, 2013.*

Whitty, M.T., Creese, S., Hodges, D., & Doodson, J. (2013 poster presentation). Who's making security risks online? *The European Congress of Psychology, Stockholm, Sweden, July 9-12, 2013.*

Whitty, M.T., Creese, S., Hodges, D., & Doodson, J. (2013, poster presentation). Who's making security risks online? *The First Annual Cyberpsychology Conference, De Montfort University, Leicester, 19th September, 2013.*

Secrets and planned lies

In Year 2, the team at Leicester completed recruitment of participants for the secrets and planned lies study. This study expands upon the work by Whitty, Buchanan, Joinson and Meredith (2012). It examines the type of medium individuals are more likely to tell their own secrets, leak other people's secrets and tell planned, serious lies to others. The types of mediums considered included: face-to face, telephone, email, instant messenger, text messages, VOIP and social networking sites. Individuals were also asked to describe the type of secret and lie they told as well as why they choose the particular medium to tell the secret or lie. In addition, we examined whether people who score high on self-monitoring or Machiavellianism are more likely to tell secrets and lies in particular medium. This data is yet to be analysed.

Avatar and image choice in online environments

Finally, colleagues at Leicester and Oxford have collaborated to construct a series of studies which examine the type of person who is more likely to use an avatar to physically represent themselves in various online spaces. Moreover, we will examine how much individuals believe this avatar represents their 'actual selves'. The first of these studies is more descriptive and exploratory, where we will investigate whether individuals select an avatar or a photograph to represent themselves in a variety of spaces. In addition, we will drill down further by paying particular attention to Facebook and twitter image choices. We will conduct a content analysis of these images as well as examine if there are any differences in personality and the types of images chosen.

5d. Current Findings: Social Acceptability Workshops

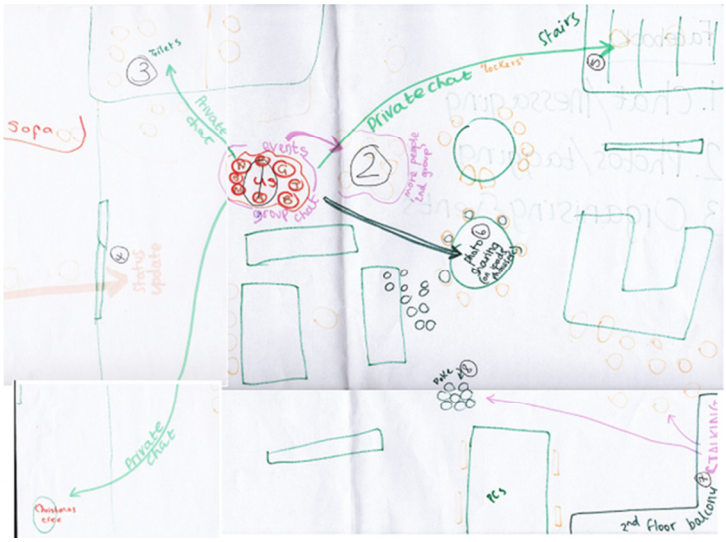
Within the CREATE lab at the University of Bath, Professor Danae Stanton Fraser and Dr Lia Emanuel have used a participatory design through a series of monthly workshops with a cohort of 13-18 year olds recruited from local schools. This group will follow the progress of the last two years of the project. They were selected given their status as high volume internet users, or what some may refer to as 'digital natives'. Yet, despite their high usage, their awareness or risks or of privacy issues has been described as surprisingly low, and there is limited research exploring teenage attitudes towards, and use of, identity information.

The focus within these workshops is to further our understanding of how young users currently perceive, experience and use identity features across physical and cyber spaces. Additionally, we use these workshops to explore the attitudes, awareness, and concerns around online disclosure in what is now a hyper-connected world.

Three workshops have now been completed with 31 school-aged students, and their findings are summarised here.

Workshop 1: Mapping Social Networks

In the first workshop, participants were asked to work in groups to draw a floor plan to depict how they visualize online social network sites (SNS) using a familiar physical environment (e.g. school, house, shopping centre). Participants were also asked to consider features they use in SNS and how these features may map on to their floor plan.



This task provided a metaphoric perspective for how participants interact and share information online through layering their experiences onto a physical environment. Importantly, this facilitated a discussion about identity in a way which drew out perceived contrasts, parallels and overlaps between online and offline interactions and provided insight into how this age group views identity across contexts and situations.

Four main outcomes emerged from this workshop:

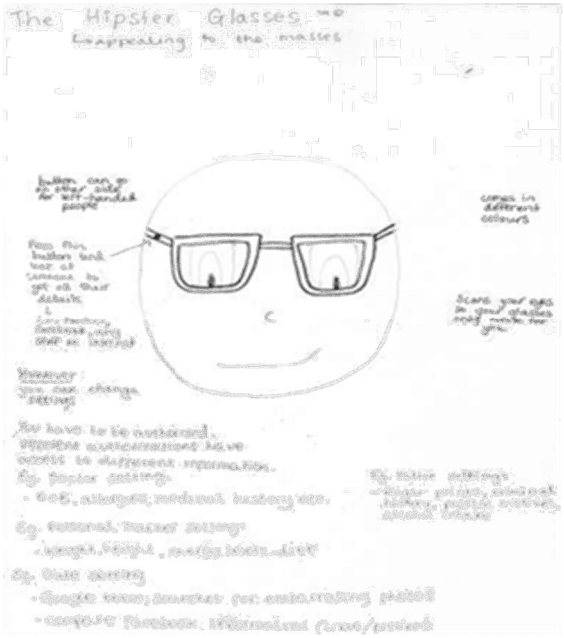
(i) First, this group outlined clear social benefits to the use of a cyber-identity that was analogous with their offline or physical-identity. This high degree of overlap may indicate that identity modelling can link cyber- and physical-attributes with greater confidence that previously considered.

(ii) Second, it was clear that this age group used many different SNS to share personal information. Moreover, they used different spaces to compartmentalise who they shared information with. Despite this, it was clear that the cyber identity across all compartmentalised spaced provided a rich identity footprint (photos, video, text, voice) which may afford subtly different snapshots of that person.

(iii)Third, some tension existed in the capacity that others may have to link information provided in the cyber domain (e.g. user name, SNS profile information) to physical world information (e.g. address, phone number) suggesting clear privacy issues within this cohort.

(iv)Finally, these teenagers clearly perceived networked mobile devices as important and possibly interchangeable aspects of interacting in both cyber and physical spaces. This was interesting and unexpected, but suggests that there may be a fuzzy boundary in the minds of these participants between cyber and physical identities.

Workshop 2: Designing future IDs



In the second workshop, participants were given the creative task of designing new forms of identification (ID) that could be implemented in the future. The workshop began by asking participants for examples of ID that 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 for banking). We also introduced examples of near-future technology such as face recognition on smartphones, RFID implants, or inferred gait mapping.

Working in groups, participants considered what type of personal information would be important to include, how their IDs would function, and how they would secure their personal information. This task enabled participants to articulate values and social considerations of new technology. Moreover, by asking participants to design a new form of future identification, their own designs acted as elicitation methods to reveal levels of awareness amongst this age group concerning identity measures and identification techniques possible now or in the near-future.

Four main findings emerged from this workshop:

(i) Teenagers showed a high level of acceptance of networked tokens, and centralised identity databases (synonymous with dataveillance).

(ii) They also showed heightened level of awareness and acceptance of biometric measures for the purposes of identification and authorization.

(iii)Teenagers perceived law enforcement bodies as one of the main end-user of new or near-future ID technologies. Participants indicated a high degree of acceptance of this perception, and of surveillance practices in general, as long as the technology was "used appropriately".

(iv)Finally, the acceptability of an identification method did not revolve around privacy or protection of information. Although participants incorporated security features in their ID designs, they judged social norms and individuality as more desirable.

Emanuel, L. & Stanton Fraser, D. (Submitted). SuperIdentity: A value-sensitive approach to explore the integration of physical and cyber identity. *In: ACM SIGCHI Conference on Human Factors in Computing Systems (CHI2014): April 26-May 1, 2014 Toronto, Canada.*

Emanuel, L. & Stanton Fraser, D. (2013). Identity and privacy in a hyper-connected world: Applying participatory design methods with young users. *First Annual Cyberpsychology Conference, 19 September, 2013, Leicester, UK.*

Workshop 3: Creating and Assessing Avatars

Within this workshop, we explored how participants portrayed themselves through avatars. In addition, we sought to understand what they thought avatars revealed about their creator. Unlike posting or sharing photographs, the user has complete control through an avatar in terms of providing as much or as little information as they wish about their actual physical features. Consequently, this approach allowed us to look at the actual behaviour and the choices participants made in what they shared about their physical identity in an online setting.

Participants were told that they would be creating an avatar anonymously and, once everyone had finished their avatar, they would be given a peer's avatar to analyse. The goal for the participants was to see what information can be derived from the avatar they were given, and to see if they could guess who had created the avatar. Prior to creating their avatars participants were asked to fill out an abbreviated version of the Interpol AM form to describe 17 of their own features. Then, participants were asked to create the avatar that best represented them. Finally, participants used the Interpol AM form once more to describe 17 features of a peer's avatar.

The discussion that followed this activity was revealing in terms of the process of avatar creation and the process of avatar judgement. The main findings were:

(i) Participants did not choose physically impossible features (e.g. purple skin or elves ears). Moreover, core, more recognisable and distinguishing features (gender, eye colour, hair colour) were relatively preserved between self-rated and peer avatar reviewed features.
(ii) Features that had a greater difference between self-reported and peer avatar reviewed across the group tended to be relatively subtle, such as lip thickness or nose size.
(iii) Many participants also incorporated non-physical aspects about themselves into their avatar (e.g., favourite colour or background picture to relate to their interests).
(iv) Overall, participants strove to make their avatars as accurate a representation as they could. One participant highlighted their reasoning behind this: "*I have like 6 different avatars for different things but I keep them all pretty similar so my friends know it's me*".
(v) Participants seemed to project this decision-making onto the wider public, stating they would have a high level of trust in the accuracy of an avatar as a reflection of the owner: "*If the avatar isn't unbelievably crazy looking…[it's] probably pretty spot on*".
(vi) Most participants felt that it would be nearly impossible to identify an individual based on their avatar. In fact, less than half (38%) of the avatars were correctly identified and matched to their creator, despite the fact that the participants were all familiar with one another.
(vii) Some tension was evident between the physical similarity of an avatar to its creator, and the capacity to identify that creator. This suggests that the use of an avatar as a means to identify someone may be viewed as socially unacceptable.

Workshop Next Steps:

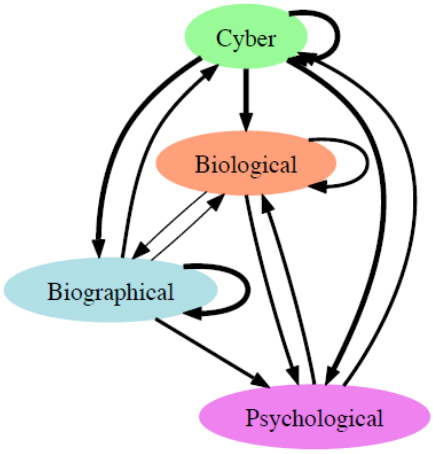
The next phase of work with this user group will focus on the perceived social, legal and ethical issues regarding the SuperIdentity model itself. In particular, we are interested in the views of the group on our ability to combine existing information or predict new information from that which is known. In addition, we also aim to explore what approaches this group may suggest as ways to address negatively perceived or unacceptable factors regarding the SID model. In this way, our participant group becomes co-designers in the SuperIdentity project.

6. The SuperIdentity Model

Responsibility for the development and refinement of the SuperIdentity model lies with Professor Sadie Creese and her team at the University of Oxford. The mathematical model is loosely based on Bayesian principles, and allows information to be combined so that logical questions can be asked. For example, given facts A and B, can I find out C?; and given a desire to find out fact C, what information do I need ? This enables the SuperIdentity team to fulfil its brief in weighting the value of information, the source of information, or the contextual influences on information. The model supports the derivation of an index of certainty to be attached to an identification decision.

The model also offers the intelligent capability to go further. Specifically, we are able to use known information to predict previously unknown information. Additionally we are able to direct information-gathering to provide alternative ways of achieving the same identification decisions and this process allows the reinforcement of previous decisions.

Within the SuperIdentity project, the model allows explicit linkage to be hypothesized, captured, and visualised between different domains of identity. In the current version of the model we use four domains – biographical information, biological information, cybermetric information, and psychological information. As well as measures in each domain potentially linking to other measures within that domain, they may also link to others measures within other domains. Most exciting in this regard is the capacity to investigate and illustrate links between the biological domain (who someone is in the offline world) and the cyber domain (who they are in the digital world).



"A model for identity in the Cyber and Natural Universes",
Hodges, D., Creese, S. and Goldsmith, M. European Intelligence and Security Informatics Conference (EISIC), 2012

"Identity attribution across CyberSpace and Natural Space",
Hodges, D., Nurse, J.R.C., Goldsmith, M. and Creese, S. International Crime and Intelligence Analysis Conference (ICIAC), 2012

Gap Analysis:

Of huge value to the SuperIdentity team has been the capacity to explore various analytics from graph theory in order to assess those identity links derived from the literature, and those that derive from the work of the SuperIdentity team. Moreover, the needs as highlighted by our canonical Use Cases, has enabled the Oxford team to perform a gap analysis in order to direct the SuperIdentity research to new and fruitful areas for research. Equally, the observation is made that this capacity to deliver a gap analysis may be of value for capability planning within an organisation, or for the wider issues of big data analytics, and personal data. Specifically, consideration has been given to whether the SuperIdentity model and capability analytics could be used to help determine policy aimed at addressing the privacy risks we may face.

Hodges, D. and Creese, S. (2013). Building a better Intelligence Machine: A new approach to capability review and development. IEEE International Conference on Intelligence and Security Informatics (ISI), 2013.

Hodges, D. and Creese, S. (2013). Breaking the Arc: Risk Control for Big Data. IEEE BigData, 2013.

Model Development:

With the model structure in place, and refined to capture our developing understanding of multi-modal identity, work in Year 2 has concentrated on two particular goals:

(i) Model enrichment, in order to support dimension and context

(ii) Model exploitation, to support different modes of operation, novel research within cyber-psychology, and innovative interdisciplinary research across the SuperIdentity project as a whole.

(1.1) Model Enrichment to include Dimensions: Whilst the SuperIdentity model was generated to operate with account of external requirements (or dimensions), it is through the Year 2 work at Oxford that we have been able to realise the capacity to nuance an identity request by these dimension. These include the capacity to make a link between fact A and fact B mindful of automate-ability, ease-of-performance, freshness-of-data, contact-with-target, maturity of link, and source-of-data. Each may be important in a given use case, and the capacity to take account of these is an important enhancement in the model's utility and real-world value.

This process of enrichment is achieved by treating each dimension as a 'type' with some fixed number of values that can be assigned. Thus, this enables the assignment of a value for any number of dimensions for each link in the model. The model is now capable of handling any number of dimensions. We currently implement two such dimensions – automatability, and link maturity – enabling the model to sort, filter and recommend routes between known fact A and unknown fact B with these dimensions taken account of.

(1.2) Model Enrichment to include Context: The concept of context is linked to that of dimensions. However, rather than specifying the conditions under which a link may be included within a solution, it specifies the environment under which the identity question is being asked. In essence, through a response to context, the Oxford team enable the model to be moulded to provide the most value for the current user in the current environment, performing the current activity with the current adversary in mind.

This ongoing development may provide a way to support an operator's use of short-cuts or heuristic approaches within the model. It may also provide support for learning and feedback loops between different operators when they are in similar contexts.

(2) Model Exploitation: The development of the SuperIdentity Model has proceeded hand in hand with the development of the Visualisation methods provided jointly by Oxford and colleagues at Pacific Northwest National Laboratories. In this regard, exploitation has focussed on the application of the model to solve tangible, real-world problems resulting in three different modes:

2.1 Defensive Mode – In this mode, the model is used to support the defence of an individual or a group's privacy, through hiding or protecting particular elements of their identity. Work has addressed this through consideration of risk at a society level from

Big Data. This, the team recognises as a socially responsible use of the model, with potential applications for the general public.

Hodges, D. and Creese, S. (In preparation). Understanding the risk to Personal Privacy in a Big Data Environment.

2.2 Investigative Mode – In this mode, the model is used to support an on-going investigation. Consider a situation in which an analyst knows one or more elements of identity and wishes to enrich this understanding with new element of identity, and with a particular unknown 'target' element in mind. This is possibly the simplest and most intuitive use of the model and is the one currently implemented by the PNNL visualisation tool.

Creese, S. et. al. (2013). Tools for Understanding Identity. Technologies for Homeland Security (IEEE: HST), 2013.

2.3 Capability Mode – In this final mode, the model can be used to encapsulate and describe an organisation's identity enrichment capability. The approach requires current capability to be recognised through the capture of enrichment tasks as inferences or links in a reasoning chain. Once the model is captured, it provides a mechanism to measure the exposure to risk should capability-loss occur (e.g. through staff movement). In addition, it may reveal the future capability development path an organisation should take, and may provide input to assist with inter-organisational collaboration and the identification of strategic partnerships.

Hodges, D. and Creese, S. (2013). Building a better Intelligence Machine: A new approach to capability review and development. IEEE International Conference on Intelligence and Security Informatics (ISI), 2013.

The Model as a Privacy Warning System

In conjunction with colleagues at the University of Bath, consideration has been given to the use of a model as a feedback mechanism regarding levels of disclosure online. Specifically, we sought to extend our understanding of users' disclosure behaviour across different social networks. Perhaps more importantly, by using the SID model as a feedback system to make users aware of the effect of individual disclosures, we explored whether users were more stringent with the information they disclosed, compared to those receiving no feedback.

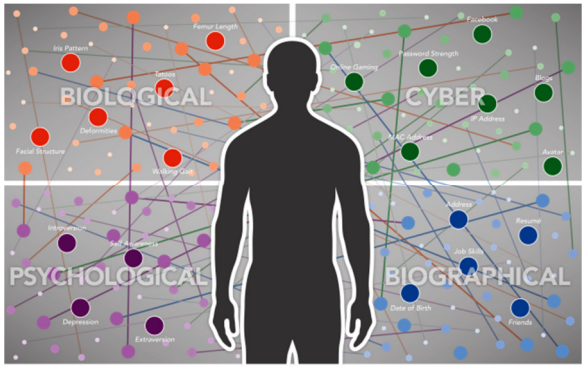
Initial results examined the privacy settings on mock social network profile pages (dating and professional network pages). The results suggested that those who received feedback via the SuperIdentity model were more conservative about how they subsequently shared biographic and work related information. However, with regard to contact and location information, their privacy settings showed little change.

The type of online space had little effect on their behaviour, or on their moderation in behaviour, and this may be surprising given that people tend to reveal different sorts of information across different online contexts. Interestingly, however, there appears to be a relationship between stringency of privacy settings and personality, with results suggesting those high in the traits 'agreeableness' and 'conscientiousness' show a higher tendency to

select more conservative privacy settings. Further analyses on the content of the social network profiles and how this changed as a function of feedback is currently underway.

Emanuel, L., Bevan, C., and Hodges, D. (2013). What does your profile really say about you?: Privacy warning systems and self-disclosure in online social network spaces. *In*: *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI2013): Extended Abstracts, April 27–May2, 2013 Paris, France.*

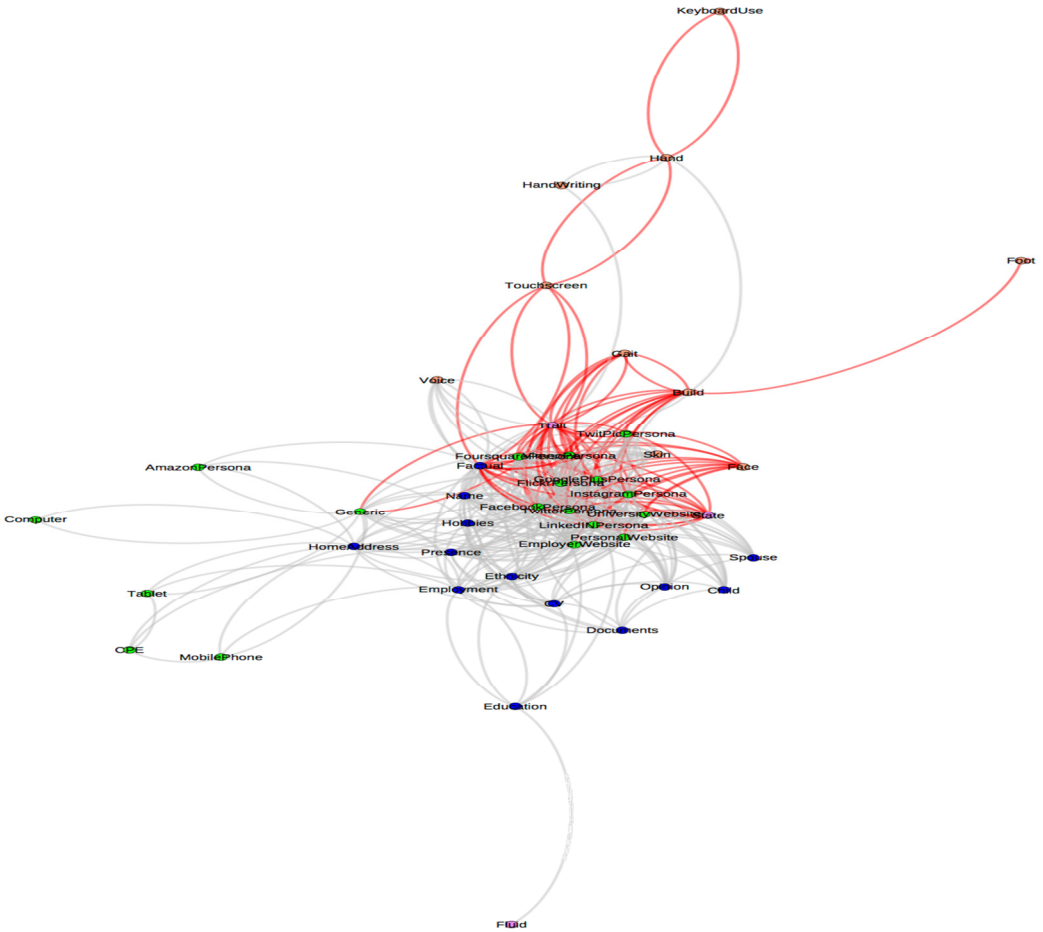
7. Visualisation



The PNNL team, in combination with colleagues at Oxford, have developed a number of frameworks within which the SuperIdentity model can be visualised. Each of the visualisation tools is guided by the needs of the user community, whilst respecting the power within the data of the SuperIdentity model itself.

The job of the visualisation interface is to represent, in an easily accessible and usable form, the research findings that sit behind the SuperIdentity concept. These take the form of the strength of a link between Identity Fact A and Identity Fact B.

A substantial literature review has identified all peer-reviewed academic research that contributes to this point. However, the SuperIdentity team is also making a unique contribution to this field through the provision of empirical tests that, together with the literature so far, augment our understanding of identity measures and their links. In fact, it is possible to from the SuperIdentity framework itself, the literature based inputs (grey), and the unique research that comes from within our team (red).

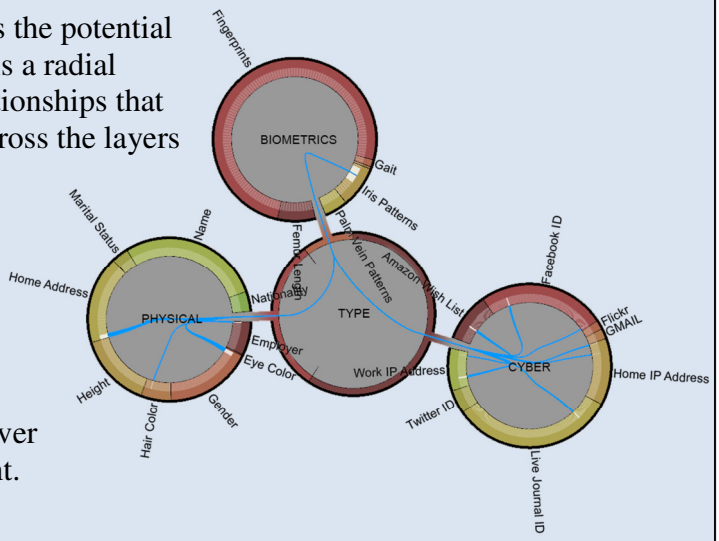


Candidate Visualisation Tools:

1. ARCWELD

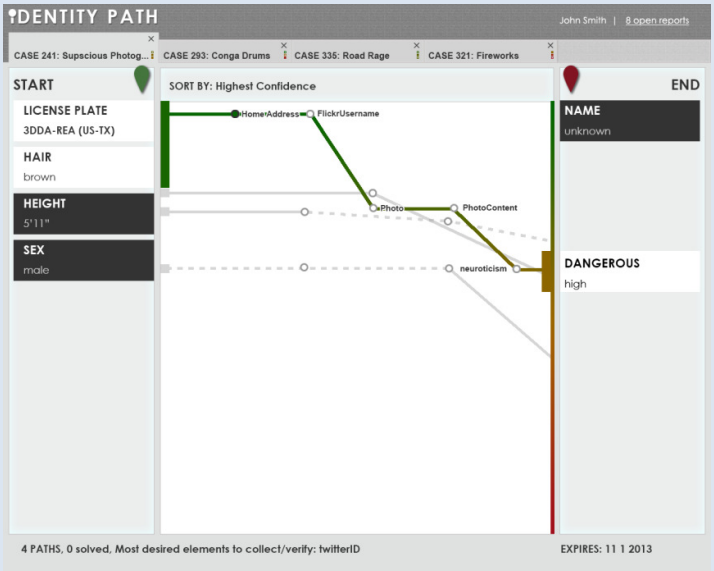
The *Arcweld* visualization emphasizes the potential of the SuperIdentity Model. *Arcweld* is a radial visualization that accentuates the relationships that may exist between elements - even across the layers of hierarchy.

By grouping elements first by their cyber, biometric and natural world designations, we can see the highly desirable transformations capable of crossing the chasms between these worlds. Digging deeper, we can discover all relationships to a particular element.



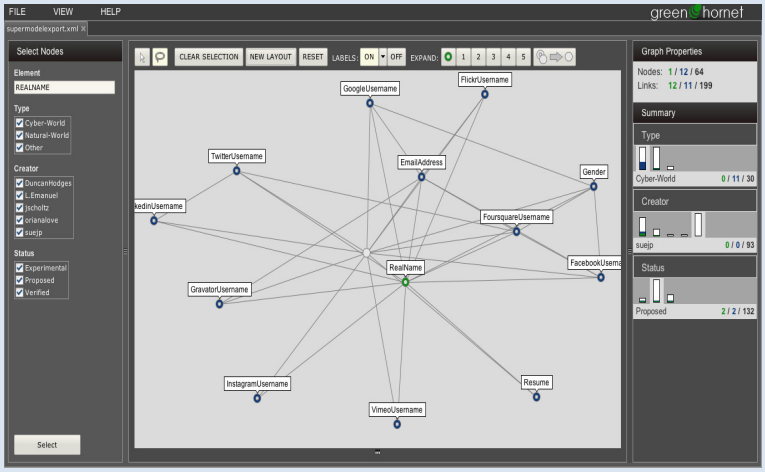
2. IDENTITY PATH

The Identity Path visualisation allows a very clear 'route map' for how to move from known fact A to unknown fact B. All possible paths can be indicated, and each can then be drilled down into in order to find the path that provides greatest certainty, the least number of steps, a chain of admissibility, or the advantage of speed, as driven by the needs of the user.



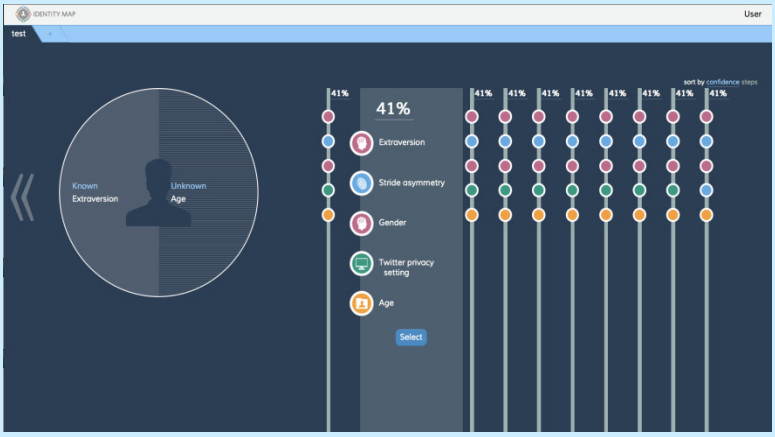
3. GREEN HORNET

The Green Hornet visualisation tool allows a web of connected information to be visualised, highlighting information that is of high value through its interconnectedness, and highlight critical yet isolated pieces of information that may enable the link to be generated between a known fact and an unknown piece of intelligence.



Selected Visualisation Tool:

4. IDENTITY MAP



Our final and chosen visualisation tool is the Identity Map, selected for its simplicity of user interface, and its customisable front end.

With input from the University of Oxford, tool-support has enabled the development of a scalable API for querying the SuperIdentity model. This abstracts a large amount of functionality away from client applications providing, for example, route-planning, basic connectivity and other functionality. With PNNL, this application supports the investigative capability mode described earlier. In addition, and in order to demonstrate the flexibility of the model, colleagues at PNNL and Oxford have built an application for mobile and tablet devices allowing users to interrogate the model to explore identity links.

On-going Refinement of Visualisation Tool:

Following input from our Steering Group, developments are ongoing to provide traffic light confidence indicators rather than an apparent quantification of confidence. In additional, development is hand to enable the tool to suggest how to enhance the identity map, and boost confidence in the destination piece of information. A critical path will be implemented, as will the capacity to select links in, or out, depending on their confidence (or lack of confidence). It is our intention to explore the capacity to work with users as design partners in the finalisation of our visualisation work.

8. Legal Input

Throughout the SuperIdentity project, the team have been advised on legal issues by Professor Steve Saxby and Ms Alison Knight from the University of Southampton. Professor Saxby is a founding member of the Institute for Law and the Web at Southampton (ILAWS), whilst Alison is a qualified Solicitor and formerly a member of the Government Legal Service. Alison works part time for the project alongside her PhD studies. A close collaborative relationship is maintained with the Information Commissioner's Office.

Monthly legal updates keep the project team advised of issues of relevance to the SuperIdentity project. These have covered 5 major themes:

Consideration of Legal issues within the SuperIdentity Use Cases:

Our User Interviews provided the SuperIdentity team with a number of US and UK-based scenarios in which identification decisions might be required. These were distilled down to provide two canonical use cases (see pp 13-14). Legal implications within these canonical use cases have been considered by the team. UK legal issues revolve around evidential impropriety and admissibility, noting a difference between surveillance activities that require prior authorisation, and non-surveillance activities, during law enforcement and intelligence investigations. Additionally issues of legal admissibility have been used to augment the visualisation capabilities within the SuperIdentity framework, so that evidential reminders can be turned on, or off, according to jurisdictional variations in law.

US Evidence note:

A thorough review of US rules of evidence provides the team with an understanding of the weight and admissibility (including standards to demonstrate relevance and reliability, authenticity and hearsay) within US federal law. This is important in terms of the capacity to use the research that sits behind SID as evidence towards identity or identification within a court of law. In particular, a review was provided regarding the legal view of electronic data. This analysis permitted conclusions to be drawn regarding whether identification by automated systems was admissible is evidence in US criminal trials.

Admissibility of Signatures in English and Welsh Law:

The brief here provides consideration of pen and ink signatures and of digital signatures. The admissibility of the latter are considered through caselaw in England and Wales. This brief provides direct advice to the SuperIdentity team currently involved in signature verification through automated means.

UK, US and Commonwealth Evidentiary Standards:

A review was provided to address the weight attached to different biometrics within a court setting. The value of this review lies in being able to inform our SuperIdentity framework of where evidence may not be admissible, and equally of where it is, and may be regarded as high value information.

Key within this analysis is consideration of caselaw, as mistakes in how evidence is used within one trial can damage the credibility of that biometric for subsequent trials. Consequently, four qualities are flagged as critical for the value of any biometric: (i) clear reliability, (ii) repeatability, (iii) acceptance according to academic peer review, and (iv) the capacity to stand under cross examination.

This analysis provides a warning for new or emergent methods of identification in terms of the standards required in order to avoid a damaged court reputation.
The review considered over 100 cases across the UK, US and Commonwealth. Whilst more traditional biometrics reflected a stable pattern of evidentiary admissibility, the review also highlighted the changes over the last 15 years in definitions of evidentiary standard, particularly in terms of the purpose of use for biometrics within court.

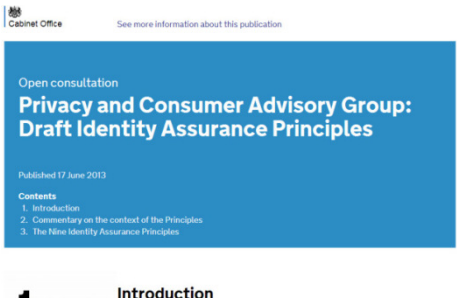
Data Handling Guidelines:

Given the undertaking of a very substantial database collection (The SuperIdentity Stimulus Dataset – SSD), the legal team provided critical advice regarding ethics, data handling and data management requirements both of the team, and of any research groups who, under licence, make use of the database. At a very immediate level, these guidelines lay out good practice for data management, and, together with Home Office input, have informed the content of the SSD licence. At a more general level, the issues inherent in data management have informed discussion of how the SuperIdentity framework can be used within current legislative bounds. Emergent issues here concern *information creep* – using information for a purpose that was not intended by the individual, *data security* and issues around the US-EU data protection *Safe Harbor agreement*, as well as updates to the *Freedom of Information Act (2000)* following the implementation of the *Protection of Freedoms Act* (2013).

The guidelines also provide possible future considerations regarding the usability of the SuperIdentity Framework from a legal perspective, with a clear reflection of the changing EU legislation regarding the European Commission's proposed new *Data Protection Regime* as it is currently being debated. If implemented, this would immediately act to harmonise data protection procedures and enforcement across the EU, including providing citizens with more rights to ensure privacy online.

In resolution, the SSD is only to be used for a set time period and under licence. That licence places responsibility with the user for appropriate maintenance of anonymity, publication of identity information only when explicit user agreement has been provided, no third-party usage or dissemination, and appropriate assurance of data security.

Forthcoming Identity Assurance Service (IAS):


Cabinet Office

See more information about this publication

Open consultation

Privacy and Consumer Advisory Group: Draft Identity Assurance Principles

Published 17 June 2013

Contents

1. Introduction
2. Commentary on the context of the Principles
3. The Nine Identity Assurance Principles

Introduction

This is to be overseen by the UK Cabinet Office's Identity Assurance Privacy and Consumer Advisory Group. IAS is intended to permit individuals security and control over the identifying information they share whilst reducing identity fraud. Nine identity assurance principles underpin the IAS framework, taking a user-centric approach:

1. user control
2. transparency
3. multiplicity
4. data minimisation
5. data quality
6. service user access and portability
7. governance/certification
8. problem resolution
9. exceptional circumstances

The briefing document reviews this development, with key points of reflection for the SuperIdentity group.

E-Crime Report:

A summary was provided of the first ever e-crime report, published by the UK Home Affairs Select Committee, following a 10 month inquiry. This includes a series of recommendations for government and industry. The report look, amongst other things, at the growth of e-crime on social networks, and considers how people can do more to protect personal data. Almost 1 in 5 people (18.4%) in the UK have had their online accounts hacked, with some people (2.3%) losing more than £10,000 due to criminal activity. This is one of the main findings of a survey on Cyber Security by members of the University of Kent's Interdisciplinary Research Centre for Cyber Security.

Saxby, S., & Knight, A. (2013). Identity crisis: Global Challenges of Identity Protection in a networked world. In Proceedings of the 8th International Conference on Legal Security and Privacy Issues in IT Law (LSPI), 11-15th November, Bangkok, Thailand.

Saxby, S., & Knight, A. (2013). The SuperIdentity Framework. 8th International Conference on Legal Security and Privacy Issues in IT Law (LSPI), 11-15th November, Bangkok, Thailand.

9. Dissemination

Online Activities

Website: www.superidentity.org (877 unique visitors)
Links to: IMPRINTS: http://www.imprintsfutures.org/links/

Project Films:
Bath: http://www.youtube.com/watch?v=MQfVKtTPlaU
Project: to be released October 2013.

Outreach and Dissemination

Black, S.M. (2013) 5 Invited talks, including the opening of Techfest

Guest, R.M. (2012). The SuperIdentity Project: exploring relationships between physical and cyber identity domains. Biometrics Institute, New Zealand High Commission, London. Sept 13th 2012.

Hodges, D. (2012). Geek Night, University of Oxford.

Stevenage, S.V., & Neil G.J. (2012). Representing yourself online. Interactive stand and dissemination materials at Community Open Evening: INTECH Science Centre, Winchester, Hampshire

Stevenage, S.V., (2012). CSI day for Year 8 students. How can you tell who someone is? Delivered to 76 Gifted and Talented local school children under the Southampton Learn with US outreach programme.

Academic Conferences

Bevan, C., & Stanton Fraser, D. (submitted). Touchscreen Biometrics: What Do Your Touch Gestures Say About You.

Creese, S., Hodges, D., Jamison-Powell, S., & Whitty, M. (2013). Relationships between password choices, perceptions of risk and security expertise. *HCI International 2013: Las Vegas, Nevada, USA, July 21-26, 2013.*

Creese, S. et. al. (2013). Tools for Understanding Identity. Technologies for Homeland Security (IEEE: HST), 2013.

Emanuel, L. & Stanton Fraser, D. (Submitted). SuperIdentity: A value-sensitive approach to explore the integration of physical and cyber identity. *In: ACM SIGCHI Conference on Human Factors in Computing Systems (CHI2014): April 26-May 1, 2014 Toronto, Canada.*

Emanuel, L. & Stanton Fraser, D. (2013). Identity and privacy in a hyper-connected world: Applying participatory design methods with young users. *First Annual Cyberpsychology Conference, 19 September, 2013, Leicester, UK.*

Emanuel, L., Bevan, C., and Hodges, D. (2013). What does your profile really say about you?: Privacy warning systems and self-disclosure in online social network spaces. *In*: *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI2013): Extended Abstracts, April 27–May2, 2013 Paris, France.*

Guest, R.M., Stevenage, S.V., He, H., & Neil, G.J. (2013). An Assessment of the Human Performance of Iris Identification" IEEE: HST conference, Boston, November 12-14th 2013.

He, H., & Guest, R.M. (2013). A Configurable Multi-Engine System Based on Performance Matrices for Face Recognition". IEEE: HST conference, Boston, November 12-14th 2013.

Hodges, D., Creese, S., &; Goldsmith, M. (2012) "A Model for Identity in the Cyber and Natural Universes," *Intelligence and Security Informatics Conference (EISIC), 2012 European* , vol., no., pp.115-122, 22-24 Aug. 2012 doi: 10.1109/EISIC.2012.43 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298821&isnumber=6298809

Hodges, D., Nurse, J.R.C., Goldsmith, M. and Creese, S.(2012). "Identity attribution across CyberSpace and Natural Space". International Crime and Intelligence Analysis Conference (ICIAC), 2012

Hodges, D. and Creese, S. (2013). Building a better Intelligence Machine: A new approach to capability review and development. IEEE International Conference on Intelligence and Security Informatics (ISI), 2013.

Hodges, D. and Creese, S. (2013). Breaking the Arc: Risk Control for Big Data. IEEE BigData, 2013.

Saxby S. (2012). The SuperIdentity Workshop. *7th International Conference on Legal, Security and Privacy Issues in IT Law* (LSPI), 2-4 October, Athens, Greece.

Saxby S., & Knight, A.M. (2013). SuperIdentity Framework. *8th International Conference on Legal Security and Privacy Issues in IT Law* (LSPI), Bangkok, 12-15th November, 2013.

Stevenage, S.V., & Neil, G.J. (2012). Knowing What you Know: Using Metamemory to Predict Accuracy of Eyewitness Identifications. *IA-IP*. 5-7 December, London.

Stevenage S.V., & Neil, G.J. (2012). The relative strength of voices and faces in person recognition. *British Psychological Society, Cognitive Section Annual Conference*. Invited talk within the Voice Recognition Symposium. 29-31 August, Glasgow.

Stevenage, S.V. (2013). Parallel modes of person identification. Invited talk within International Voice Recognition Symposium, 21-22nd November, Brussels, Belgium.

Whitty, M. (2013, April). Who am I: Identity across different cyberspaces. *Cyber Security Seminars: University of Oxford, April 25, 2013.*

Whitty, M. (2013, September). Keynote address: Who am I? Is identity consistent across physical and cyber spaces? *The First Annual Cyber-Psychology Conference, De Montfort University, Leicester, September 19, 2013.*

Whitty, M. T., Creese, S., Hodges, D., Doodson, J. (2013). (poster presentation). Who's making security risks online? *The European Congress of Psychology, Stockholm, Sweden,* 9 July – 12 July, 2013.

Whitty, M. T., Creese, S., Hodges, D., Doodson, J. (2013). (poster presentation). Who's making security risks online? *The First Annual Cyber-Psychology Conference, De Montfort University, Leicester, September 19, 2013.*

Academic Publications

Bevan, C., & Stanton Fraser, D. (submitted). Touchscreen Biometrics: What Do Your Touch Gestures Say About You.

Black, S.M., Creese, S., Guest, R.M., Pike, B., Saxby, S.J., Stanton Fraser, D., Stevenage, S.V. and Whitty, M.T. (2012) SuperIdentity: fusion of identity across real and cyber domains. In, ID360 - The Global Forum on Identity, Austin, US, 23 - 24 Apr 2012.

Black, S.M., MacDonald-McMillan, B. & Mallett, X. (2013). The incidence of scarring on the dorsum of the hand. Int J Led Med DOI: 10.1007/s00414-013-0834-7.

Black, S., MacDonald-McMillan, Mallett, X., Rynn, C. & Jackson, G. (2013). The incidence and position of melanocytic nevi for the purposes of forensic image comparison. Int J Leg Med. DOI: 10.1007/s00414-013-0821-z

Hodges, Duncan; Creese, Sadie; Goldsmith, Michael (2012) "A Model for Identity in the Cyber and Natural Universes," *Intelligence and Security Informatics Conference (EISIC), 2012 European* , vol., no., pp.115-122, 22-24 Aug. 2012 doi: 10.1109/EISIC.2012.43 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298821&isnumber=6298809

Jackson, G. & Black, S. (2013). Use of data to inform expert evaluative opinion in the comparison of hand images – the importance of scars. Int J Leg Med. DOI: 10.1007/s00414-013-0828-5.

Neil G.J., et al. (final draft) The Southampton Stimulus Database: Physical, digital and psychological measures of identity.

Robertson, J., & Guest, R.M. (2013). A feature based comparison of stylus and finger based signature characteristics. In: Proc: IGS 2013, Nara, Japan, June 2013

Saxby S.J., & Knight, A. (2013). Identity crisis: global challenges of identity protection in a networked world. 8th International Conference on Legal Security and Privacy Issues in IT Law (LSPI), Bangkok, 12-15th November, 2013.

Stevenage, Sarah V., Neil , Greg J., Barlow, Jess, Dyson, Amy, Eaton-Brown, Catherine and Parsons, Beth (2012) The effect of distraction on face and voice recognition. Psychological Research, 77, (2), 167-175. (doi:10.1007/s00426-012-0450-z). (PMID:22926436).

Stevenage, Sarah V., Hale, Sarah, Morgan, Yasmin and Neil, Gregory James (2012) Recognition by association: within- and cross-modality associative priming with faces and voices. British Journal of Psychology (In Press).

Stevenage, Sarah V., Neil, Gregory James and Hamlin, Iain (2013) When the face fits: recognition of celebrities from matching and mismatching faces and voices. Memory (In Press).

Whitty, M. T., Bevan, C., Emanuel, L. L., Neil, G. J., Jamison-Powell, S., Stanton-Fraser, D., Stevenage, S. V. (under review). Who am I? Self-concept across Facebook, dating sites and LinkedIn.

Lay Publications

Stevenage, Sarah V., Whitty, Monica and Saxby, Steve (2013) Who am I? [in special issue: Complexity: a New Way to See the World] International Innovation, 2013, 82-84.

Planned Books

Saxby, S., Black, S.M., & Stevenage, S.V. (Eds.) Legal Reflections on Digital Identity.