ID360 Paper Summary Form

Please include this form as the first page of your submitted paper.

Paper Title:
SuperIdentity: Fusion of Identity across Real and Cyber Domains

Author Information

Name: Sue Black, Sadie Creese, Richard Guest, Bill Pike, Steve Saxby, Danaë Stanton Fraser, Sarah V Stevenage*, Monica T Whitty

Affiliation: *University of Southampton

Email: *svs1@soton.ac.uk

Phone #: +44 2380 592234

ID 360 Dimension (may select more than one):

√ Law √ Technology √ Society Policy Business

Keywords:
Identification, Verification, Biometrics, Cyber-Identity

Application Area or Market Sector:
Intelligence, Security

Abstract:
Under both benign and malign circumstances, people now manage a spectrum of identities across both real-world and cyber domains. Our belief, however, is that all these instances ultimately track back for an individual to reflect a single 'SuperIdentity'. This paper outlines the assumptions underpinning the SuperIdentity Project, describing the innovative use of data fusion to incorporate novel real-world and cyber cues into a rich framework appropriate for modern identity. The proposed combinatorial model will support a robust identification or authentication decision, with confidence indexed both by the level of trust in data provenance, and the diagnosticity of the identity factors being used. Additionally, the exploration of correlations between factors may underpin the more intelligent use of identity information so that known information may be used to predict previously hidden information. With modern living supporting the 'distribution of identity' across real and cyber domains, and with criminal elements operating in increasingly sophisticated ways in the hinterland between the two, this approach is suggested as a way forwards, and is discussed in terms of its impact on privacy, security, and the detection of threat.

SuperIdentity: Fusion of Identity across Real and Cyber Domains

Sue Black[1], Sadie Creese[2], Richard Guest[3], Bill Pike[4], Steve Saxby[5],
Danaë Stanton Fraser[6], Sarah V Stevenage[*7], Monica T Whitty[8]

1. Centre for Anatomy and Human Identification, University of Dundee
2. Department of Computer Science, University of Oxford
3. School of Engineering, University of Kent
4. Pacific Northwest National Laboratory, US
5. The Law School, University of Southampton
6. Department of Psychology, University of Bath,
7. Psychology, University of Southampton
8. Department of Media and Communication, University of Leicester

* Corresponding author

IDENTITY: ITS CHALLENGES

Identity is a complex concept, reflecting issues of stability, context, privacy and ownership, across real and virtual media. The goal of identity assurance, together with the consequences that follow when identity cannot be assured, has become the focus of significant efforts both within the UK government, and further afield. Despite the fact that it is likely to be an underreported crime (Whitty & Buchannan, in press), identity fraud is estimated to cost £1.96 billion per year in the UK alone (Annual Fraud Indicatory, 2011). In addition, cyber-security is named in the top 5 threats to national infrastructure. Taken together, these facts underline the view that research in this area is both timely and urgent. The purpose of the present paper is to explore the concept of identity at the level of the individual, and to explore the challenges that surround identity and identification as we move towards an ever more digital age. A novel approach – SuperIdentity – is presented, together with considerations for identity research looking forwards.

For the purposes of the present paper, we define identity as a label or concept that distinguishes one individual from another - in essence, it refers to 'who you are'. The goal of identity assurance models is to verify a particular identity from a set of given biometrics. Some qualifications to this basic definition are, however, required. First, it is clear that whilst identity is a stable biological fact, 'who you are' at a psychological level is dependent on a host of factors such as who you are with, what role or task you are currently fulfilling, and who you see yourself as at a certain point in time. Identity can be seen as quite fluid, and identity then becomes an issue not merely of 'who you are', but of 'who you are *now*'. Models of identity assurance are generally concerned with the former of these definitions, so that the right people gain access to required information, services, or systems. Increasingly, however, such models cannot ignore the latter definition. Indeed, failure to do so would run the risk of failing to recognise that apparently different 'identities' belong to the same individual.

The concept of 'multiple identities' (e.g., Gergen, 1991; Markus & Nurius, 1986; Turkle, 1997) has been used within Psychology and may be of value here. This concept recognises that an individual may simultaneously occupy a number of real but different roles, each of which is an accurate reflection of an aspect of themselves even though they may be quite distinct from one another in name, behaviour, membership of social group, etc. Consider, for example, an individual who is an office worker by profession, a member of the gym and a supporter of the local football club for recreation, and a parent in the playground at the end of the school day. Allied to this is the concept of 'partial identity' which has been used within Computer Science (Rannenberg, Royer & Deuker, 2009). Here, the emphasis is on the fact that identity may be revealed through many different fragments which, when amalgamated, approach a complete sense of who someone might be. This carries with it the benefit of increased trust from individuals who are then capable of verifying their identity whilst maintaining minimum disclosure. Within this paper, we prefer the term 'distributed identity' and use this to capture both the fact that we can occupy different roles across contexts, and that each role can be revealed through fragments that combine to make up the whole. This leads to our first research premise: *A complete sense of identity requires a combinatorial approach.* Without this, isolated pieces of information give an incomplete and disjointed perspective of the person.

An additional consideration that cannot be ignored, and that sets an important context for the current work, is the impact of technology on identity. In a recent text by Sullivan (2011) it is noted that our digital identity can exist in numerous forms and can be used for a rapidly increasing set of purposes from national databases, to online transactions, to social communications across richly populated networks. Digital identity has come to be used as a commodity to buy services, access, information, or rights in the way that physical currency may have been used in the past (Crosby, 2008). Not only does this mean that we have a broader base across which to distribute our identity, it also means that we have a broader set of threats against which to protect our identity, or within which to assure our identity. This leads to our second research premise: *A complete sense of identity requires acknowledgement and understanding of the digital or cyber context as well as the real-world context.*

CURRENT SOLUTIONS:

In the field of identity assurance, several solutions already exist and these have generally but not exclusively been tasked with identity authentication rather than identification. In the physical domain, considerable work has been conducted within the fields of automated biometric recognition and human biometric recognition, and this has traditionally taken a uni-modal approach. This work has focussed on a variety of biometrics including the face, voice, fingerprint, iris, gait, and more recently, ear measurements (Jain, Ross & Prabhakar, 2004). The goal of this work has been to establish the reliability of each marker as a stable biometric, and to benchmark the accuracy of recognition that follows. In the near future, anthropological knowledge might be expected to underpin the development of new and robust authentication techniques. In this regard, an understanding of the aetiology of a physical feature may enable both an appreciation of its stability and maturation rate, and its correlation with existing and emerging physical or behavioural biometrics. As an example, this may include closer scrutiny of the hand both in terms of its geometry and vein patterns. As measures, both are relatively visible and socially accepted biometrics to obtain, but their value for authentication purposes, and their correlation with other potential biometrics, has yet to be fully tested (Black, Mallett, Rynn & Duffield, 2009).

In the digital domain, usernames, passwords, and responses to user-specified prompts serve as the common basis for identity authentication. Further security can be added through a two-factor system, requiring the user to have possession of a token and knowledge of a fact. To use a banking example, the user requires the bank card *and* knowledge of its associated PIN. However, these measures carry a cost for the user both in terms of the retention of information, and the fraudulent use of information for malign purposes. The highest level of security may depend on three factors: possession of a token, knowledge of its key, and proof by biometric of the right to use it. In contrast to these approaches, more consumer-driven solutions are worthy of note. Whilst often providing a lower level of security by making use of the answers to user-specified questions that could be extracted or guessed from online profiles (e.g. what is your favourite colour?), these solutions nevertheless have the benefit of increasing user trust, user engagement with the system, and user involvement in policing its access.

Importantly, online identity is not limited to electronic usernames, passwords, or online responses. The concept of cyber-identity is important in this regard, and this might be illustrated by how an individual chooses to present themselves in an online forum such as a dating site, or what they decide to self-disclose in a chat room. Cyber-metrics will capture aspects of these cyber-identities, and these form an exciting and relatively new addition to our identity toolkit. Indeed, given that identity can be revealed in digital as well as physical contexts, cyber-metrics are a necessary addition to emergent models of identity and identification. Cyber-metrics may include information such as online browsing behaviour, usage of social network sites, online profiles within games or groups, or online styles of interaction that may reveal identity even when a user tries to hide it. This represents an emergent field for researchers, providing the opportunity to explore how identity is expressed and managed online.

In this regard, interesting debates are taking place regarding the similarity of online versus real-world identities in terms of the extent to which one may be useful in predicting the other. For example, there is considerable interest in the extent to which individuals trust online or cyber services, with questions being raised both across individuals (i.e., the internet generation versus an older generation) (Gilleard & Higgs, 2008; Nie & Erbring, 2000), and within individuals (Cityware project, University of Bath). Taking wifi hotspots as an example, research on trust and security of online systems revealed that messages which are partly generated by users, and partly generated by systems, may give people confidence that ad-hoc associations between their personal devices and urban pervasive services are secure (Bevan, Mitchell, Kindberg, O'Neill, Grimmett, Stanton Fraser & Woodgate, 2011). The perception of trust was also improved both through the perception of exclusive access to information (Kindberg, Bevan, O'Neill, Mitchell, Grimmett & Woodgate, 2009), and through the use of visual cues to improve apparent authenticity through depicting the exclusive location of the service (Kindberg, O'Neill, Bevan, Kostakos, Stanton Fraser & Jay, 2008).

Alongside this, online trust of a different nature has also been explored – trust in the user. Turkle (1997), for example, discusses online deception in the form of alternative 'cyber-selves' and the effort of pretence. He notes how one's self-perception can change as a result of deception, with consequences when 'simulation bleeds into reality'. More recent work by Whitty, Buchannan, Joinson & Meredith (2012) has explored deceptive behaviour both online and offline with a view to exploring whether intuitive fears are confirmed and deception is more prevalent online. Through a diary study, they found that lies were more likely to be spontaneous rather than planned, and were aimed more at those who are close to us or to complete strangers. Interestingly, these researchers found that whilst planned lies tended to be told via SMS, most spontaneous lies occurred over the telephone rather than online as had been feared. Where we lie, they suggest, is in part determined by the 'features' of the communication (including how recordable, distributed, synchronous, personal or 'lean' the communication is considered to be by the user). Whilst this literature is still relatively young, it offers the capacity to explore a critical piece of the identity puzzle – the linkage between identity in a cyber and a real world context.

COMBINATIONS OF INPUTS

A number of projects have begun to address the more ambitious question of combining information in pursuit of a more robust means of authentication or identification. For example, the Future of Identity in the Information Society (FIDIS), an EU funded network of excellence set up in 2004, comprised academics from multiple disciplines within 13 Member States. It was created following an acknowledgment by the European Information Society (EIS) that our traditional notions of identity have been challenged, particularly in light of the digitisation of information. FIDIS's primary objectives were to provide an integrated approach to research on identity and identity management, and to shape future requirements for their management within the EIS. Following five years of research FIDIS's output shaped the interdisciplinary approach necessary to address identity management, profiling, protection, and legal implications, and raised considerable challenges surrounding security and trust, as well as privacy concerns (http://www.fidis.net/home/).

The recently completed EU co-funded project "STORK 1.0" (Secure idenTity AcrOss BoRders LinKed) was rather more practical in its objective. It sought to extend existing national electronic public services, by providing access to these services by citizens across the EU. Through a European eID interoperability platform, citizens requiring access to public service(s) within their nation state, but who are resident or situated in another participating Member State, are now able to authenticate themselves online, using their national electronic identity ("eID"). As authentication from the citizen's government can be obtained through the platform, the need for physical presence is removed, thus transactions can be conducted in a secure manner across borders with greater ease and efficiency. The success of STORK relied upon the mutual recognition of eID between participating states. Other than its clear benefit to citizens seeking to work, live and study in different EU countries, STORK also 'claims to provide a focal point for electronic identity initiatives in the EU…' (https://www.eid-stork.eu). The authentication process across combination of electronic metrics has provided clear benefit over reliance on a single indicator of identity, but at present it is only capable of checking electronic metrics against a database of established and acceptable eID measures and this gives rise to a lack of generalisability and, at present, a failure to scale.

Alongside these online identity projects, the combination of inputs has also become more prevalent in biometric research. Automated solutions combining data from multiple metrics such as the face, voice and fingerprint, improve overall identification rates (Jain, Nandakumar & Ross, 2005) albeit with additional computational overheads as a result. Such multimodal systems work either by combining the *features* from multiple modalities, *recognition results* across a series of single metrics expressed as % matches to a target, or *recognition results* expressed as simple binary match/no match outcomes. Performance can, however, be improved through the use of 'meta-data' – a term used to denote all the additional information known about either the individual or the biometric which sets a context within which it can be assessed. For example, known biographical information such as age or gender of an individual can narrow a search-space or tune a classification system to a population sub-group. Likewise, information about the quality of, or conditions under which, a measure was recorded may be used to predict confidence in the identification that can result (Grother & Tabassi, 2007).

Data quality issues may be especially important in the context of growing interest in automated biometric systems capable of recognising individuals from *unconstrained* or sub-optimal inputs (Ruiz-del-Solar, Verschae & Correa, 2009). At present, there is a clear and measurable deterioration in performance under these more ecologically valid conditions. However, this performance decrement may be offset by the adoption of a combinatorial approach incorporating additional inputs to supplement what might be considered 'idiosyncratic' or unconstrained inputs.

In this regard, a very exciting development is represented through recent work to combine physical and digital aspects of identity. This was conducted by the Cityware project, which developed methods for combined human and electronic observation. Human characteristics were recorded (e.g gender, age range) whilst wireless scanning enabled digital data capture and classification. Characteristics of both the devices and the people carrying them (such as whether their data were generated from mobile phones or notebook computers) were recorded, while Bluetooth names provided a further identity marker that enabled classification beyond conventional observational methods (O'Neill, Kostakos, Kindberg, Fatah gen. Schiek, Penn., Stanton Fraser & Jones 2006). Notwithstanding this, we note a significant gap in our understanding of the linkage of identity metrics across real-world and cyber contexts. In this regard, potential exists for the development of an identity framework based on a rich combinatorial model across multiple measures and contexts.

A CHANGE IN THINKING

Achievements in the area of identity are evident and noteworthy, changing the way that both identity assurance and identity management have been viewed. However, rapid changes in the way that we are now able to express (and modify) our identity require that our understanding of identity moves forward to keep pace. The most significant area for development is now in the area of cyber-metrics to indicate identity in an online space, and challenges emerge not only because the opportunity for self expression is so great, but also the scope for deception is arguably increased. It is our contention, though, that a rich understanding of cyber-metrics must not sit in isolation of the biometrics that exist in the real world. Instead, work is urgently called for to understand how measures of real world and online identities may be linked. The SuperIdentity project addresses this gap in thinking through a novel interdisciplinary collaboration to push forward a rich understanding of modern identity.

THE SUPERIDENTITY PROJECT

The SuperIdentity project (SID) is an innovative and exciting approach to the concept of identity. The assumption underlying this project is that, whilst there may be many dimensions to an identity - some more stable than others - all should ultimately refer back to a single core identity – the source or 'superidentity'. In this sense, we propose a rich combinatorial model with identity metrics that span both the real-world biometrics and the online cyber-metrics. Our purpose is to provide intelligence and law-enforcement services with a greatly enhanced ability to identify individuals both within and across real and cyber domains. SID deviates from existing approaches in three notable ways:

(i) SID represents contributions from an *expansive spectrum of scientific domains*, enabling a broader set of identity measures to be considered than in previous work. The measures on which we focus reflect static and behavioural cues from both the real world and the cyber world to formulate a cutting-edge exploration of identity. The addition of behavioural measures enhances SID by incorporating temporal and dynamic information so that identity can be represented as more than a set of static measures. Furthermore, the integration of cyber measures enables longevity of the concept so that SID not only addresses short- and mid-term issues, but will still be a viable model in the longer term. As perhaps the fastest growing identity domain, and the fastest changing means of self-representation, the inclusion of cyber-metrics is an area that both current and future approaches must address with some urgency.

(ii) SID represents the capacity to *combine a rich set of identity measures* with clear benefit in terms of the robustness of the identity model and the resultant identification process. Whilst a combinatorial modelling approach exists for often self-contained sets of real-world measures, it has never been used with cyber measures and it rarely bridges traditional domains. In this regard SID uses tried and tested capabilities but with a novel configuration of inputs.

A combinatorial approach has the capacity to result in articulation of the minimum amount of information required so that a user can meet a determined threshold for an effective identification. This is an important consideration both in a legal and ethical sense. Within such safeguards and constraints, SID can progress with awareness of the need for trust, assurance, and social acceptability in the minds of the public.

A combinatorial approach may also enable detection of patterns or correlations between measures. In this sense, known measures may predict other previously unknown measures of identity. To use a marketing example, the prediction of one thing given another is common practice. Consider for example, an e-commerce analyst who examines data correlations within shopping preferences to suggest that an individual who buys Product *X* might also like Product *Y*. It is possible also that one piece of identity based information may similarly be correlated with, and so predict, another. For example, measures of physical identity from the hand may highlight relationships between anatomical features that were not previously appreciated, such as keyboard strokes, kinetics, or area of fingerprint left at a scene, and in the context of a paedophile investigation, video imagery may then be linked with online chat room behaviour or forensic analysis at a scene. This is a very new approach providing fertile ground to examine the predictive relationship between one identity measure and another.

(iii) Finally, SID provides the capacity to *quantify the certainty* associated with an identification through weighting each measure according to its reliability in a given situation. This latter point is important. Faces, for example, hold high value when making an identification, but are of limited value when disguise, occlusion, pose, or lighting impair vision or image-capture. By weighting inputs according to their reliability in a given context, SID will be able to prioritise measures in a combinatorial space, and this may provide a response to instances in which multiple data points are contradictory. The outcome will provide a ‘sensitivity analysis’ that describes the value of each measure of identity, helps to recognise and resolve contradictions, and is useful for targeting data-collection towards the most effective measures.

In combination, SID provides *fusion* of known measures, *revelation* of unknown measures, and *quantification* of certainty associated with each measure and thus the identification decision overall. In this way, it provides a step-change in the way that we think about identity and identification and the value that it might hold for the real world.

MOVING FORWARDS

Three avenues of investigation have been beyond the scope of this paper, but we recognise them as being important in terms of the changing concept of identity. The first concerns the overlap that exists between online and real-world expression of identity, and the predictive capacity that each can hold for the other. The second concerns the rapid expansion in the use of cyber-identity information to support consumerism, in what has become known as the monetisation of identity. The third concerns the use of cyber and real-world intelligence to inform identity at the level of the organisation, the group, or perhaps the ‘cell’ of criminal activity. All avenues share a reliance on an interface between real and cyber identity.

In terms of overlap between online and real-world expressions, one clear example is provided through an individual’s choice of icon or avatar. Given that an individual may choose or create an avatar of any description, natural questions emerge in terms of the extent to which an individual’s avatar resembles their real identity. This, of course, is hugely determined by the context in which the avatar is used. Nevertheless, the question remains as to whether characteristics of the individual in the real world can predict characteristics of the individual as represented through their avatar, and vice versa. Early literature in this area suggests that psychological wellbeing may be correlated with resemblance to avatar such that those whose avatar deviates most from their ideal self may be most unhappy (Bessiere, Seay & Kiesler, 2007). Allied to this is a valuable discussion exploring not only physical resemblance but behavioural resemblance between avatar and real life (Whitty, Young & Goodings, 2011). Whilst there is a considerable literature on this, and whilst avatar choice represents only one example of cyber-physical overlap, these issues underline the importance of a research agenda which examines the expression of identity across real and cyber contexts, and the predictive value of each for the other.

In a similar vein, by viewing identity as a monetised quantity, we note again the interplay between real and cyber identities. In particular, the extent to which cyber space has driven forward this monetisation may be evidenced through the movement towards highly targeted advertising. In essence, the more information you can gather on an individual the better you can sell to them, requiring an ability to uniquely identify the facets of identity that reveal personal preferences. Social networking environments, and apps on smartphones, are currently providing a wealth of data, and the constant move towards proliferation of sensors and instrumentation of the data means that there will be a certain expansion of the elements of identity which might be gathered in cyber space. Again, a research agenda which is focussed on the linkage of identity across real and cyber space will be the only way we will be able to keep pace with the use of identity information for consumerism.

Finally, by considering identity at a group level we note the need for a fundamental shift in level of abstraction, if we are to link individuals into groups and assure those linkages across time and space. In this regard, the capacity to link real-world biometrics and cyber-metrics is again critical. Indeed, linkage or affiliation between group members may be denied in one context but evident in another. For example, in the London riots of 2011, individuals’ behaviour from visible real-world metrics may have suggested the riots to be the acts of an apparently random group. However, online activity on social networking sites showed these individuals to be associated and organised in their behaviour. Interviews with user groups will be instrumental in understanding the questions that users may want to ask of this information, and the ways they may want to visualise or tailor their capabilities in this regard. Looking forwards, an augmented reality visualisation tool would be perfectly placed to enable the appreciation of identity at a group level, especially where the individuals within a single group may be scattered in a physical space, but may be highly associated and strongly linked in a cyber space. This may be of value in terms of the detection of threat within a crowd scene such as a football match, an airport, or a state visit. However, it may equally hold value in revealing links between individuals in a group spread across national or even global locations.

CONCLUSIONS

Within this paper, a broad reflection has been provided on the current context of identity research. The SuperIdentity or SID model has been outlined as a way to move forward in this field, emphasizing in particular the value of an approach which combines a rich set of measures from real and cyber contexts in a way that enables confidence and predictive validity to be determined. We also recognise a number of fruitful avenues for future research, each of which depend on the linkage of information across real and cyber domains. Without this, research will not keep pace with the changing face of identity expression and identity management, and we will fail to capture the full extent of identity, or protect ourselves from a motivated threat against it.

REFERENCES

Annual Fraud Indicator. (2011). National Fraud Authority, Home Office. http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2011?view=Binary. Last accessed 26.02.1012.

Bevan, C., Mitchell, J., Kindberg, T., O'Neill, E., Grimmett, J., Stanton Fraser, D., Woodgate, D. (2011). Influence of User Choice on Perception of Wireless Connection Genuineness and Security. Proceedings of the First Workshop on *Pervasive Urban Applications (PURBA) in conjunction with the Ninth International Conference on Pervasive Computing (San Francisco, June, 12-15).*

Bessier, K., Seay, F., & Kiesler, S. (2007). The ideal elf: Identity exploration in World of Warcraft. *Cyberpsychology and Behavior, 10(4)*, 530-535.

Black, S.M., Mallett, X., Rynn, C. & Duffield, N. (2009). Forensic hand image comparison as an aid for paedophile investigations. *Police Professional*, *184*, 21-24.

Crosby, Sir J. (2008). Challenges and Opportunities in Identity Assurance. www.hm-treasury.gov.uk

FIDIS NoE: Future of Identity in the Information Society: http://www.fidis.net/home/ (accessed 23 February 2012).

Gergen, K. (1991). *The Saturated Self: Dilemmas of Identity in Contemporary Life*. New York: Basic Books.

Gilleard, C., & Higgs, P. (2008). Internet use and the digital divide in the English Longitudinal Study of Ageing. *European Journal of Ageing, 5*, 233-239.

Grother, P. & Tabassi, E. (2007). Performance of Biometric Quality Measures, *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4)*, 531-543.

Jain, A., Nandakumar, K. & Ross A. (2005). Score normalization in multimodal biometric systems, *Pattern Recognition, 38(12)*, 2270-2285.

Jain, A., Ross, A., & Prabhakar, S. (2004). *An Introduction to Biometric Recognition.* IEEE Transactions on Circuits and Systems for Video Technology. Special Issue on Image- and Video-Based Biometrics, 14(1), 4-20.

Deleted: .

Kindberg, T., Bevan, C., O'Neill, E., Mitchell, J., Grimmett, J., & Woodgate, D. (2009). Authenticating ubiquitous services: a study of wireless hotspot access. In Proceedings of the 11th international Conference on Ubiquitous Computing (Orlando, Florida, USA, September 30 - October 03, 2009). Ubicomp '09. ACM, New York, NY, 115-124.

Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Stanton Fraser, D., & Jay, T. (2008). Measuring trust in wi-fi hotspots. In Proceeding of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems (Florence, Italy, April 05 - 10, 2008). CHI '08. ACM, New York, NY, 173-182.

Markus, H., & Nurius, P. (1986). Possible Selves. *American Psychologist, 41(9)*, 954-969.

Nie, N.H., & Ergring, L. (2000). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society.

O'Neill, E., Kostakos, V., Kindberg, T., Fatah gen. Schiek, A., Penn, A., Stanton Fraser, D. & Jones, T. (2006). Instrumenting the city: developing methods for observing and understanding the digital cityscape. In *Proc. UbiComp 2006,* Orange County, California, USA, ACM. 315-332.

Rannenburg, K., Royer, D., & Deuker, A. (2009). *The Future of Identity in the Information Society: Challenges and Opportunities*. Springer: Dordrecht, London, Heidelberg, New York.

Ruiz-del-Solar, J., Verschae, R., & Correa, N. (2009). Recognition of Faces in Unconstrained Environments: A Comparative Study. *EURASIP Journal on Advances in Signal Processing (Recent Advances in Biometric Systems: A Signal Processing Perspective)*, 2009, Article ID 184617.

SSEDIC: Single European Digital Identity Community: http://www.eid-ssedic.eu/

STORK: Secure Identity Across Borders Linked: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=55&Itemid=76#stork_faq_2 (accessed 23 February 2012).

Sullivan, C. (2011). *Digital Identity: An Emergent Legal Concept*. University of Adelaide Press.

Turkle, S. (1997). *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster.

Whitty, M.T. (2008). Revealing the ‘real’ me, searching for the ‘actual’ you: Presentations of self on an internet dating site. *Computers in Human Behavior, 24*,1707-1723.

Whitty, M.T., & Buchanan, T. (in press). The online dating romance scam: A serious crime. *CyberPsychology, Behavior and Social Networking.*

Whitty, M.T., Buchanan, T., Joinson, A.N., & Meredith, A. (2012). Not all lies are spontaneous: An examination of deception across different modes of communication. *Journal of the American Society for Information Science and Technology, 63(1)*, 208-216.

Whitty, M.T., Young, G., & Goodings, L. (2011). What I won’t do in pixels: Examining the limits of taboo violation in MMORPGs. *Computers in Human Behavior, 27*, 268-275.

ACKNOWLEDGEMENTS

This project is funded by the UK EPSRC (EP/J004995/1) with support from the US Department of Homeland Security. Our thanks go to the entire project team, with special thanks to Chris Bevan, Rachel Fletcher and Duncan Hodges for helpful comments in preparation of this manuscript. Our thanks also go to Tom McCutcheon and Richard Allen for help during the formation of these ideas.