A day in the digital life: a preliminary sousveillance study

Fletcher, G, Griffiths, M and Kutar, M

A Day in the Digital Life: A Preliminary Sousveillance Study

Gordon Fletcher
Salford Business School
University of Salford
M5 4WT
United Kingdom
g.fletcher@salford.ac.uk

Marie Griffiths
Salford Business School
University of Salford
M5 4WT
United Kingdom
m.griffiths@salford.ac.uk

Maria Kutar
Salford Business School
University of Salford
M5 4WT
United Kingdom
m.kutar@salford.ac.uk

Abstract

A decade ago, Castells argued that most surveillance would have no directly damaging consequences. He proposed that what should be of more concern were the unpredictable consequences of our over-exposed lives, the lack of explicit rules for on-line behaviour and how this then was interpreted by a 'multitude of little sisters' who process and store this information, forever (Castells 2001:180). A decade later, these conjectures are still valid but are now at a critical level as individuals passively volunteer personal information while government and commercial organisations aggressively amass these snippets into correlated data. As boundaries between on-line and off-line blur, and geo-locative applications grow in popularity, we echo Castells by asking, what will be, and what are, the privacy implications of existing in a technologically saturated environment? The human data trail now begins prior to conception and continues after death. We aim to develop a methodology to enable us to quantify this trail and to examine the impact that such amassment of data has on society, communities, and personal identities within the UK. The reality is that the digital footprint is a significant research challenge to identify and then quantify. There is a critical need to capture relevant activities in a holistic and interconnected manner in order to enable understanding of the societal implications. We describe a preliminary study which will be used as a starting point to develop appropriate methods for quantification and analysis of the 21st century digital footprint.

Finding the Digital Footprint

There is a lack of established functional research methodologies that provide sufficient structure or clarity of resolution to aid the collection and analysis of data surrounding individual digital footprints. Attempting to track and document an individual's digital footprint requires a high degree of methodological pluralism given that data is drawn from a diverse range of digital and analogue settings. As researchers we will be (re)turning the gaze back onto those watching, data harvesting and monitoring society by examining the decentralised and uncoordinated methods employed to collect personal digital data. Thus this study becomes an inverse surveillance or 'sousveillance' exercise[1]. The major focus of this preliminary study is to develop methods to capture individuals' digital footprints as they use and come into contact with Internet, surveillance, communications and database technologies over a 24-hour period. We have employed a broad range of technologies to detect and identify this footprint including GPS, phone records, key-logging software, video technology, as well as direct observation in an endeavour to interrogate all of the digital activity a person generates, initiates or is associated with over this brief period of time.

By combining a blend of critical and virtual ethnographic approaches (Cecez-Kecmanovic 2001; Hine 2000) we report on the process of capturing two individuals' exposure to digital and surveillance technologies over a 24 hour period. The approach is at least partially inspired by the exploratory 'garbage' studies of Rathje and Murphy (2001). In this earlier work, first conducted in 1973 in Tuscon, the examination of discarded material items assisted in determining actual consumption patterns rather than those conventionally reported through subsequent surveying or forms of direct participant observation. We

[1] Mann, S. (2005) Sousveillance and Cyborglogs: A 30-Year Empirical Voyage through Ethical, Legal, and Policy Issue, Department of Electrical and Computer Engineering, University of Toronto

can then identify, categorise and describe the shape of a personal digital footprint and attempt to establish which elements of a digital footprint are stored by commercial or governmental organisations. Further work will include graphically mapping this footprint in conjunction with researcher and artist Heath Bunting[2], who has developed an identity mapping toolkit as a result of his own concerns and interests around this topic. We aim for these actions to become a starting point to develop both a repeatable methodology and a clearer understanding of the consequences of the rapid and uncritical adoption of public digital technologies for individual privacy and identity. In an attempt to unravel the closely entwined notions of privacy and identity this paper is organised at follows: we first discuss the concept of privacy and surveillance technologies, From this point we then endeavour to isolate identity and present a number of definitions or terms of reference of identity, digital footprint that will be adopted for this study. We introduce Heath Bunting's work and present the design, development and the investigational process of the Day in the Digital Life (DDL) study. The paper closes with a discussion on the complexities of designing a workable methodology and how findings from this research process will be incorporated into the future work to capture individual Days in the Digital Life.

Privacy in a Technologically Saturated World

Wajcman (2002) claims that societies across the world are experiencing historically, unprecedented change as they try to adapt to a more interconnected but highly uncertain world (2002: 347). It would be reasonable to append to Wajcman's observation that the pace of change has intensified in the subsequent decade in a multitude of technologies and activities, all of which are increasingly 'networked' and producing still greater levels uncertainty. Recent examples such as the 'Arab Spring', near ubiquitous social networking, and both the CCTV-led response by the constabulary to the UK riots as well as the subsequent "I love my city" campaigns can all be regarded as indicative of this observation. The current study focuses its attention, amongst all of these examples of change and uncertainty, upon the notion of privacy and the growth of surveillance against the backdrop of a heavily technologically mediated social world.

Privacy as a concept is a conundrum. Individuals knowingly, continuously and willingly allow individual pieces of personal data to be collected – their Personal Identifying Information (PII). This data can then be extensively profiled and distributed amongst third parties who are often authorised to receive this data through permission given by checking (or failing to uncheck) the tick box on a term and conditions form or hidden – in plain sight - within the text of privacy policies. However, in a recent study, O'Donnell et al (2010a) argue that surveillance should not be judged directly as either good or bad as its perception is influenced by additional factors. They (O'Donnell et al 2010a) focus upon the way in which perceptions of surveillance are affected by contextual influences directly relating to the form and location of the surveillance. For example, increased workplace surveillance through data-logging and CCTV monitoring has a direct impact on productivity and overall job satisfaction. By using social identification theory to understand the source of surveillance and how identification with that source impacts upon the acceptability of surveillance, they found that those who do not identify or have a different social identity, view surveillance as an invasion of privacy but those that share a sense of social identity are much more likely to accept surveillance practices and technologies. Surveillance practices produce a distinctive dichotomy from which it is individually difficult to disentangle the competing factors. Taken negatively, surveillance is seen as a form of societal control that reduces personal liberty for little or no benefit to the individual's being surveilled and entirely for the benefit of those who control the means to monitor. The most optimistic opinion sees surveillance practices and technology as beneficial by providing a constantly present additional form of security that offers protection to law abiding citizens and their property. Wells and Wills (2009) explore an alternative inconsistency in the debate regarding individualism and identity, by exploring the context of surveillance practices made possible by prevalent speed camera technologies. In this study (Wells and Wills, 2009), self-ascribed respectable non-criminal drivers are threatened by the risk that speed camera technologies may construct their identities as deviant and potentially even criminal. They found that punitive speed camera monitoring practices introduced the concept of '*othering*', that groups

[2]Heath Bunting's Status Project: http://status.irational.org/visualisation/maps/

perceived as deviant by 'respectable' drivers were more worthy of surveillance attention rather than ‘me’. In effect, the presence of surveillance technology is regarded by individuals who perceive their own practices as 'correct' as being for 'others' and effaced from their immediate concern or consideration. Our own study, to amass an individual’s digital data trail over a 24 hour period, builds upon the understanding developed through existing surveillance studies to highlight and attempt to quantify the extent and intensity to which all individual's within the UK are under surveillance.. With a more accurate survey of the forms and extent of surveillance in the UK – a clearer and more accurate understanding of this phenomena will assist in empowering those who are being surveilled. However, this empowerment has the consequence of diminishing existing power relations and is at least one partial explanation for the degree to which identifying and quantifying existing surveillance technology is so difficult With increased knowledge of the forms and practices of surveillance, society has the tools to radically alter their behaviour as a response. However, the most realistic response will be a continuing low level of societal concern (Bhargav-Spantzel et al, 2007), the response that continues to most support the societal power of those who surveil.

Concerns regarding data privacy and the degree to which surveillance technology concentrates power within a small number of public and private organisations are more than offset by the societal desire for immediacy. As a society, we demand information at our fingerprints, become impatient if we have to wait more than moments to receive authorisation for a financial transaction, and increasingly find it disconcerting and even abhorrent if required information is not available electronically and are required to wait for any form of information to be received through the postal system. To facilitate this requirement for the immediacy of information, authentication and access controls requires a two-way exchange of PII. Individual demand for instant access to information requires virtual interaction that will also necessitate that a number of personal attributes have to be voluntarily relinquished. Bhargav-Spantzel et al (2007), refer to a variety of studies that demonstrate a strong relation between user’s privacy attitudes and their behaviour towards digital interactions. From this comparative work Bhargav-Spantzel et al (2007) identify three character types in relation to privacy. *Privacy fundamentalists* will register to websites giving inaccurate, incomplete data, and are concerned about privacy threats favouring governmental regulation of information data. *Pragmatists* have an objective privacy attitude and balance the risks to their privacy interests by what benefits they receive for the sharing of the Personal Identifying Information (PII). The third type is the *Unconcerned* individuals who have little or no anxiety about their digital privacy, concerns are usually associated with the level of PII required, and Bhargav-Spantzel et al (2007), suggest that biometric or health data factor higher than simple demographic data. Bendle (2002) warned in 2002 that the acquisition and management of identity in a technological driven world, is vital but equally problematic. Shirley Turkle, in 1995, with what could now be described as a simplistic perspective, was enthusiastic about the prospect for individuals to express multiple and often unexplored aspects of the self, to play with their identity and to try out new ones (Turkle 1995, 12).

Invisible Networks

Existing literature in the fields of privacy, surveillance and information systems discuss issues relating to identity with a variety of definitions available for the cluster of terms relevant to the work described here. See, for example, Clarke (1994), Parsell)2008), Tavani (2011) and Toekke (2011). In particular, ‘identity’, ‘digital identity’, ‘digital footprint’ are used variously in a range of contexts with subtly differing meanings These terms are central to the presentation of the work described in this paper and so we provide clear definitions of what we mean here by each term. The pilot project described in this paper has further highlighted the need to distinguish between the ‘types’ of data recorded, stored and processed with differing levels of direct input required from the direct actions of the individuals who relate to the data.

Identity can be most broadly defined as a characteristic which enables entities to be distinguished from one another; this is equally applicable to human beings, organisations or data structures. Our need to identify, distinguish and classify entities has different motivations and drivers. For human beings the primary driver for articulating an identity is to define one’s relationship to others. At a personal level it is closely associated with definition of ‘self’ and consequently the relationship that ‘self’ has with ‘other’. This interconnection is reflected in popular definitions of ‘identity’ such as “characteristics that somebody recognizes as belonging uniquely to himself or herself and constituting his or her individual personality for life” (Encarta Dictionary). In relation to discussions of surveillance and a digital footprint it enables a

person to define a relationship to the differing loci of social power (e.g. government, organisations and institutions such as banks etc). This enables differentiation from other human beings and for records to be created, updated and maintained that provide a log of interactions, exchanges and decisions. A persistent recurring feature in traditional definitions of identity is the notion that 'identity' is also a conferment of uniqueness. Historically, this is suggestive of an unambiguous one-to-one relationship between a human being and their identity. There have always been cases of individuals with multiple identities but in the analogue world these deviations represented a tiny fraction of the total pool of individuals and identities. An emergent but key issue that has developed in the digital era is the ability for people to create and maintain different highly differentiated identities in different spheres of their lives. This issue is outside the scope of this particular paper but is noted as being of significance relevant to our wider project.

We draw on the innovative work of the artist Heath Bunting and in particular his *Status Project* in defining terms relating to identity. The *Status Project* surveys the component features of identity and produces maps of influence and personal portraits. Bunting's work distinguishes three kinds of person; the 'human being', the 'natural person' and the 'artificial person'. The 'human being' represents the physical embodiment of the person, the flesh and blood homo sapien. The 'natural person' is defined as "A transferable bundle of rights and duties that can be attached to only one human being". The attachment of a natural person to a human being enables the individual to manage their role in society, allows the individual to be managed, and is important as the enabler of commerce and other functions. The artificial person is defined as "A transferable bundle of rights and duties that can be attached to one or more natural person(s) or one or more artificial person(s) or both, e.g. a corporation". The 'artificial person' generally relates to collectivities of human beings, and is typically a corporation, although there are some individual roles or institutions which require a notion of succession and that are consequently defined as artificial persons including monarchs, bishops, lords mayor and so on.

These definitions of 'persons' are useful in both digital and analogue worlds of experience as they facilitate an explanation as to how individuals simultaneously hold multiple identities; whilst a natural person can relate to only one human being, in the opposite direction one to many relationships are possible and so the human being may, in theory, be attached to more than one natural persons. This reflects Clarke's (1994) concept of the 'digital persona' which he defines as "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual." However we distinguish our notion of identity from that of Clarke's digital persona. In the contemporary digital world, it is increasingly difficult for individuals to separate the public and private realms of experience. The rise of social media in particular has seen a convergence between what has been previously seen and discussed as separate spheres of life. Although it is possible for an individual to maintain different personas, this must be explicitly managed through formation and maintenance, a quite different situation from the time where an individual's roles could be more easily distinguished and compartmentalized. We therefore use a definition of identity as being *'a set of characteristics which are unique to a single human being'*. This is similar to Bunting's definition in that it is unidirectional, such that an identity may only relate to a single human being, but it is possible for a human being to hold more than one identity, reflecting, for example, the use of specific identities on social media sites. Unlike Bunting however, we do not refer to rights and duties in our definition as the work here is concerned with measurement and quantification of identity rather than with specific discussions of control, rights or authority. At birth, a human being becomes an identifiable individual, but the set of data items needed or used for identification is only a subset of those which relate to that individual. When an individual is a few hours old they might be identified by the hospital that they are in by the date and time of their birth plus some other unique identifier such as NHS number, hospital number, name of mother etc. However for babies in the digital world, these items comprise a small subset of the total dataset that can be attached to and assist in defining their identity. At a time when the average age of digital birth is 6 months and almost a quarter of children appear online following their first sonogram / ultrasound scan (Businesswire 2010), by the time a human being is physically born, the dataset relating to their emergent identity might include medical records, photographs of ultrasound scans, websites and even unique communicable social media identities.

As with the problematic and contested use of the term 'identity', various loosely defined terms have been used to describe the data trail left behind by individuals in the digital era. These include 'digital footprint', 'Internet footprint' and 'data trail' and each focuses upon or emphasises a specific relationship between

technology and the individual. These terms are often used to refer to both transitory and more persistent data, as well as explicit and implicit transactions of data. Our experience in attempting to quantify the data relating to an individual over a 24 hour period has highlighted the importance of distinguishing and classifying these different types of data events in a manner that acknowledges their relationship to the human being. When examining the digital evidence of an individual's life and how this evidence is generated there are many components which may be identified. These might include triangulated mobile phone and GPS data, Internet usage, direct recording on CCTV cameras, the data generated through a credit card transaction or the swiping of an access card. There are both transitory and persistent elements to each data event but significantly each can be explicitly tagged to an individual. For the purposes of data surveillance it is the persistent elements of the data event that are significant and meaningful, however, greatest concern regarding the exposure of private data relates to the transitory aspects of the event – for example, the security of the connection for a website login or observation by a third partner when using a cash machine. It is also significant to acknowledge that in building a picture of the full set of data events in an individual's day, it is also necessary to incorporate those events that are disconnected from the direct immediate actions of the human being, that were initiated through actions in the past and that still continue to influence the totality of data that is daily generated relating to that individual. For example, many banking transactions, including 'automatic' ones such as the processing of direct debits and standing orders can occur regularly, creating a data event that exists primarily within the systems of a bank and the receiving organisation. An appointment might be generated by a Doctor's surgery or the results of a medical test might be received which would then result in updates being made to the record held remotely from the individual.

We utilise two further definitions to further position the Day in the Digital Life project; 'digital footprint' and 'digital identity'. We define a digital footprint as "the real time data generated relating to an identifiable individual' and digital identity as the 'historical digital footprint'. Any individual data event (for example sending an email or logging into a Facebook account), will create a digital footprint, but most aspects of this data event will be transient. It is primarily the smaller amounts of persistent data that is left behind and ultimately stored in a remote database that will evoke some form of change, no matter how small, to the individual's digital identity. A data event is analogous to placing a footprint in wet sand. The step itself begins to immediately dissolve but more permanent changes may be preserved deep below, buried beneath the surface. The digital footprint is the most obvious and immediate indicators of an individual's digital interactions. An individual's digital identity is stored across a network of servers and databases which in many cases will contain relationships that have been subsequently defined by sophisticated third-party interrogation of accumulated personal persistent data. Digital identity then is the totality of an individual's identity within the digital and encompasses all of the digital personas utilised by the individual with a temporal span that exceeds the human life to which it relates.

Recording a Day in the Digital Life

Design considerations

In considering a methodological framework for this study we were mindful of the problematic nature nexus of digital data, identity, privacy, surveillance and ethics. This is an awareness that is well-documented by recent literature. boyd (2010) states that 'privacy is completely intermingled with Big Data' and that social media sites such as *Google and Twitter* are amassing 'terabytes of data about human interactions'. Solove (2004) similarly warns of the compilation of 'digital dossiers' by businesses and governments (boyd 2010; Solove 2004). Zittrain (2008) adds a further dimension to Solove's (2004) initial warning by adding that it is not just government and multi-national businesses that are capable of capturing data. The ready availability of cheap digital technologies including peer-to-peer networking, GPS recording and IP-cameras are facilitating alternative active participation in the capturing of surveillance data in a manner that he describes as Privacy 2.0 (Zittrain 2008).

Capturing the totality of data events that occur during a Day in a Digital Life is the primary methodological challenge of our research. However, equally challenging is the secondary need to identify and record in a useful manner the persistent and hidden aspects of a digital identity in this 24 hour period. The key to our

design was to create an approach that was repeatable with minimal researcher intervention and with commonly available technologies. The goal was to create a methodology that would enable the research to be conducted at a much greater scale by willing participants at a wide variety of location across different periods of time. This desire itself proved challenging, in part because 'commonly available technologies' are part of the power relationship to individuals and their usage of this technology. The Apple iPhone (or at least one that is not jail-broken), for example, proved to be of only minimal utility to the project and primarily as a recording device for external interactions – the network traffic facilitated by the iPhone proved too literally be a 'blackbox' unless it was tethered to a desktop computer running the phone's debug terminal.

Design of pilot

The pilot for the research involved designing the mechanisms that would gather the entire range of an individual's data events that occurred in a 24 period with a minimum of intrusion. Any additional equipment would, and did, produce additional data events. It was also necessary to develop a design that recognised that certain types of events would not be immediately apparent and would require subsequent, possibly significant, retrospective research. We enrolled two participants who were both willing and aware of the range of the intersecting issues between privacy, identity and surveillance and assigned them different days of the week for their digital day. Both participants were equipped with a low-power but accurate GPS tracker and a head mounted miniature (Looxcie) camera as well as a Flip video camera as a backup. The focus upon gathering visual information reflected the sousveillance aspect of the research with the goal of capturing the image and location of the devices that generated data events regarding an individual that were beyond their own volition. The first participant also agreed to install a stealth keystroke monitoring software application onto their PC. In their briefing both participants were encouraged to utilise their mobile phones as an additional recording device and asked not to delete any activity logs from their PCs or phones. Many of these decisions subsequently presented challenges to the research and data analysis. Most significantly, our design emphasised capture of the transient aspects of data events which, while indicative, also revealed the degree of difficulty of identifying and retrieving the persistent aspects of data events. However, this was anticipated tentatively in the need for a sense-making stage to the research that was conducted between the participants and researchers following the 'field' work. Many of the issues that were raised during the actual 24 hour periods of data gathering reinforced the need and importance for sense-making but equally presents a wider issue for the creation of a methodological approach that is repeatable and scalable.

Post-24 hour sense-making

Following the 24 hour pilot period of data gather we conducted a debrief session attended by the two participant researchers and the three members of the project team. The majority of the tools used to capture data were seen to have been suitable for their specific data gathering duties; GPS recorder, mobile phones and spyware software had all been efficient and unobtrusive. Participants had been happy to provide explicit records during the pilot, including sending geo-located tweets showing sousveillance in action, and using voice recordings to highlight notable events during the actual day. The most problematic area was the video recording; the Looxcie camera that was provided sits behind the ear but there were a number of problems with this piece of hardware; moreover the participants felt uncomfortable and 'obvious' in wearing it and so alternatives will be sought for future iterations of the study. Participating in the study had heightened the participants' sense of awareness of digital interactions but had not unduly influenced their general day-to-day behaviour (beyond the explicit actions required to record their activities). However, some elements of their activities required explicit intervention to ensure that they were recorded – this was particularly the case for interactions with surveillance technologies and it became clear that passive sousveillance of these cannot be achieved.

A Day in the Digital Life: Version 2

In order to track and capture the complexities of interaction and trails that are left as part of a digital footprint and their subsequent impact on the construction of digital identity, we endeavoured to capture the totality of 24 hours of digital activity by two individuals. Our initial inspiration for approaching this

challenge was the garbage studies of the 1960s. This earlier work closely echoed many of the goals of our own research in the ways that it sought to understand the day-to-day relationship of individuals to each other and organisations through observations made of the remnants left by their day-to-day activities. Taking this perspective still further, the 'Vegemite' study in Australia in the 1990s attempted to understand everyday life through detailed interviewing of individuals about their consumption habits and daily practices provided useful guidance in designing a large scale project that captured detailed data regarding personal activity. Our challenge in focusing on the digital aspects of everyday life was the inaccessibility of data without the mediation of various electronic devices – whether it was a conventional desktop, a laptop computer, a mobile phone or a cashpoint (ATM). From this point of view we were working with the assumption that evidence of the extent and content of their digital footprint would be available as digital but nonetheless tangible and discrete remains. Our research preparation consequently used a rhetoric that reflected this notion; 'capture', 'store' and even 'get'. Our research kit similarly took on this worldview with storage devices of various types – hard drives, cameras, GPS loggers – in order to retain the various 'things' that might be generated around and by the research participants and that would be actively retrievable.

The perhaps overly naïve assumption that the project would be endeavouring to gather tangible digital 'things' that were 'left' by individuals as a consequence of their direct actions shaped the way in which we briefed our researchers. Retrospectively the methodology requires further tools to capture a more expansive topography of an individual's activities. Digital footprints are shaped by real time digital data events that occur at a specific moment and place such as texting, CCTV capture, ATM activities, on-line banking. Therefore digital identity is shaped by the historical digital footprint even if the digital footprint episode happened moments ago. Servers, data centres, and transparent networking link historical digital events together further adding to and continuously appending to the digital identity. Our research – DDL: Version 2 – will take up these challenges and take a wider focus with two key dimensions being added to the existing methodology. Firstly we have recognised that it is necessary to include a comprehensive baseline of digital identity prior to the start of the 24 hour data capture. This will be achieved by utlilising Heath Bunting's relations of data items that contribute to the construction of identity. In effect, Bunting's work presents a checklist of activities that shape digital identity but that do not occur 'in plain view'. This work provides a baseline that will enable us to examine and record the hidden digital episodes that form parts of the digital footprint and effect consequential change to the digital identity. To be as unobtrusive as possible we will need to reexamine the tools of everyday life and the ways in which these tools can be employed to meet the needs of sousveillance. In effect, we will need to make mobile phones – most likely an Android based phone – capable of transparently recording the digital aspects of a 'day'. The Daytum (daytum.com) project while primarily a manual and necessarily obsessive process provides us with some guidance in this direction. Nicholas Feltron's life has been quantified over the last 6 years in this manner. The challenge for our DDL project is to ensure the capture of both the transitory and persistent elements of data events that occur both locally and remotely from an individual.

Conclusion: What do we know?

Our research, to date, does not move significantly away from the dystopian prospects of Orwell's *Big Brother* or Castell's 'little sisters'. The challenge for our wider study is to explore the entire genealogical network of complexities surrounding data events and their persistent remote storage that arise from one 24 hour period of activity in the contemporary media- and technology-saturated environment of the UK.. The completed pilot work has revealed the complex interactions that exist between the constructions of the digital footprint and digital identity. This recognition has led us towards a change of emphasis within the project which will produce future iterations that will examine not only the transient data activities we personally and directly generate as we interact in a technologically saturated world, but also the persistent and underlying construction of digital identity and the consequential feedback impact that this identity has on lived experience. Capturing this totality of the loop will move us a step closer to the overarching aim of the project – to quantify the digital footprint so that we may know its impact upon digital identity and our experiences of everyday life. 'Privacy is dead, deal with it,' Sun MicroSystems CEO Scott McNealy is reported to have declared over a decade ago. Last year Zuckerburg announced that 'privacy is no longer the social norm' (2010).

Do these cavalier comments from two influential global thinkers who have been instrumental in shaping our current technological environment require a formulated and reasoned response? Is the lack of broad social resistance to current surveillance regimes an indication that they are generally recognised as normal and acceptable? Are contemporary changes to the accepted notions of privacy and surveillance a short-term realignment as digital identity becomes an embedded aspect of the broader concept of identity?

What we have already shown from our preliminary research is that surveillance is an ever present constant in UK everyday life irrespective of an individual's uptake of technological tools. The concerns regarding the gathering of personal data by third parties, if any are expressed at all, tend to focus on the visible but transitory aspects of digital surveillance. While there is cause for concern regarding this data collection these debates generally camouflage the wider ranging issues surrounding the collection and maintenance of interlinked persistent datasets that brings together events triggered directly by an individual alongside those events that occur 'elsewhere' away from any physical presence. The existence, let along the specific structure and form, of these data sets are currently beyond the reach of conventional research methodologies. Without direct access the goal of our research will be to interpolate their presence from our own ability to conduct sousveillance.

References

Bendle, M. (2002), The Crisis of 'Identity" in High Modernity, British Journal of Sociology, 53(1): 1-18.

Bhargav-Spantzel, A., Squicciarini, A., Young, M. and Bertino, E., (2007), Privacy Requirement identity Management Solutions' in Editors MJ Smith, G. Salvendy: Human Interface, Part II, HCII 2007, LNCS 4558, 694-702, Springer-Verlag Berlin Heidelberg.

boyd, d. 2010. "Privacy and Publicity in the Context of Big Data." *WWW.* Raleigh, North Carolina, April 29.

Businesswire (2010) Accessed August 2011 at http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World

Castells, M. (2001), The Internet Galaxy: Reflections on the Internet, Business and Society. Oxford: Oxford University Press.

Cecez-Kecmanovic, D. (2001), Doing Critical IS Research: the Question of Methodology. In Qualitative Research in Information Systems: Issues and Trends (Trauth, E. Ed.), pp.142-163, Hershey, PA: Idea Group Publishing.

Clarke, R. (1994) The digital persona and its application to data surveillance. The Information Society 10(2), 77-92.

Hine, C. (2000) Virtual Ethnography. London: Sage.

Johnson, B. (2010), Privacy no longer a social norm, says Facebook founder, The Guardian, accessed in August 2011 from http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

O'Donnell, A., Jetten, J. and Ryan, M. (2010a), Who is watching over you? The role of shared identity in perceptions of surveillance', European Journal of Social Psychology, 40, 135-147

O'Donnell, A., Jetten, J. and Ryan, M. (2010), Watching over your own: How surveillance moderates the impact of shared identity on perceptions of leaders and follower behaviour, European Journal of Social Psychology, 49, 1046-1061.

Parsell, M. (2008), Pernicious Virtual Communities: Identity, Polarization and the Web 2.0. Ethics and Information Technology, 10:1, 42-56.

Rathje, W. and Murphy, C. (2001) ‘Rubbish: The Archaeology of Garbage’, Tuscon : University of Arizona Press.

Solove, D. (2004), The Digital Person: Technology and Privacy in the Information Age, New York University Press and London

Tavani, H. T., (2011) Ethics and Technology: Controversies, Questions and Strategies for Ethical Computing. 3rd Edition. Wiley

Wajcman, J. (2002), Addressing Technological Change: The Challenge to Social Theory, Current Sociology, 50(3): 347-363, London: Sage Publications.

Wells, H. and Wills, D. (2009) Individualism and Identity: Resistance to Speed Cameras in the UK. Surveillance and Society 6(3): 259-274.

Zittrain, J. (2008), ‘The Future of the Internet and How to Stop It’, Yale Books, Unbound, Yale University Press. Accessed 28-08-2011