

Digital Footprints and Employability

A critical examination of the implications of digital identity with reference to the growing corporate and state use of data regarding employees

By

Diana Dupree Bsc (Hons)

Abstract

“If you drop a frog into a pan of boiling water it will leap out. However, if you put a frog in a pan of cold water and gradually increase the heat until it is boiling, it will stay there until it is scalded to death...sometimes we need to be aware of things that creep up on us before it is too late!” (Stomm cited in Öqvist, 2009, p1)

You may consider that you have a right to personal privacy. However if you regularly use the internet you will inevitably leave digital footprints: small records of your interaction which may be far from private, and which may collectively have an unwanted impact on your future. The growth of Web 2.0 technologies, such as social networking and blogging, has made it easier to digitally interact with our friends, family and others. The messages we leave behind in our own name, or in discussion with or about others can all be linked together to form a virtual shadow or online profile. Data collated about our personal lives from other digital sources such as CCTV, medical and criminal records, and information we provide government agencies, add to this profile at each interaction and can persist beyond our control. This creeping abuse or potential abuse of our privacy is often incremental and not normally noticed until it is too late to manage.

There is growing evidence (Career Builder, 2008) that employers are increasingly utilising the internet to gain ‘value added’ information on candidates, and are using this new information to eliminate applicants based on what they find. This project aims to make the reader aware of how their personal interaction with the internet could affect their future employability, and provide some guidance on how to manage their online profile. When sharing personal information online, we should do so in an informed way: With an awareness of how that information may be interpreted, potentially years into the future, by an external party, who may have an agenda far beyond the context in which we originally shared our information. The ubiquity of digital data storage and the ease of collating or linking diverse sources of data containing information about us, presents new moral and social issues which will impact our lives in ways we may not only find surprising, but also potentially damaging (Dessimoz et al, 2006).

Keywords

Web 2.0; digital footprint; virtual shadow; employ; privacy; identity

Acknowledgements

Firstly, I would like to thank my fellow students for providing support, and Linda Jones of the University Library for her initial inspiration following a lecture on the “Dark Side of the Internet” (Jones, 2008).

I would also like to thank my project supervisor and course leader, Peter Millard, for all his assistance and encouragement. Without his direction and leadership the project would have been a completely different beast.

Finally, I have to thank my husband for his unfailing support and encouragement during some particularly difficult times. He has not only provided me with emotional support during the writing of this project, but has been my rock throughout my University education from initiation to completion.

Table of Contents

1 Introduction.....	6
1.1 Background.....	6
1.2 Research Questions.....	8
1.2.1 What Is Web 2.0 And Why Is It So Important?.....	8
1.2.2 What Is A Digital Footprint?.....	8
1.2.3 What Is A Virtual Shadow And How Is This Relevant To Workplace Surveillance?.....	8
1.2.4 Is There Evidence That Prospective Employers And Recruitment Agencies Utilise The Internet For Background Checks On Applicants During Any Recruitment Process?.....	8
1.2.5 Can Some Employee Interaction With Web 2.0 Applications Be Beneficial To Business?.....	9
1.2.6 What Personal Data Is Stored And Potentially Used By The State Within The UK And Globally With Regard To The Workplace?.....	9
2 Web 2.0 And Digital Footprints.....	10
2.1 What Is Web 2.0?.....	10
2.1.1 The History.....	11
2.2 Digital Footprints And Virtual Shadows.....	13
2.3 Web 2.0 Applications.....	14
2.3.1 Social Networking.....	14
2.3.2 Blogging.....	16
2.3.3 Wiki's.....	16
2.4 The Future And Web 3.0.....	17
2.5 Chapter Summary.....	18
3 Corporate Use Of Personal Internet Data.....	19
3.1 Generation Google.....	19
3.2 Dataveillance And The '24 Hour Employee'.....	20
3.3 Employee Recruitment And Internet Presence.....	21
3.4 Examples Of Employment Problems Associated With Internet Presence. .	22
3.5 Personal Internet Use At Work.....	23
3.6 Social Networking For Business.....	25
3.7 Chapter Summary.....	26
4 The Law, The Government And Corporate Access To State Data.....	27

4.1 E-Government.....	27
4.1.1 Data Snooping.....	28
4.1.2 National Databases.....	29
4.2 Law Relating To Privacy And Identity.....	32
4.2.1 Data Protection Act, 1998.....	32
4.2.2 Regulation Of Investigatory Powers Act, 2000.....	34
4.3 Chapter Summary	35
5 Fieldwork.....	36
5.1 Methodology.....	36
5.1.1 Primary Research.....	36
5.2 Results.....	36
5.3 Fieldwork Methodological Critique.....	36
6 Discursive Review And Examination Of The Implications Of Digital Identity.....	38
6.1 Corporate Use Of Personal Internet Data.....	39
6.2 The Law, The Government And Corporate Access To State Data.....	43
7 Conclusion.....	46
7.1 Research Questions.....	46
7.1.1 What Is Web 2.0 And Why Is It So Important?.....	46
7.1.2 What Is A Digital Footprint?.....	46
7.1.3 What Is A Virtual Shadow And How Is This Relevant To Workplace Surveillance?.....	46
7.1.4 Is There Evidence That Prospective Employers And Recruitment Agencies Utilise The Internet For Background Checks On Applicants During Any Recruitment Process?.....	47
7.1.5 Can Some Employee Interaction With Web 2.0 Applications Be Beneficial To Business?.....	48
7.1.6 What Personal Data Is Stored And Potentially Used By The State Within The UK And Globally With Regard To The Workplace?.....	48
7.2 Project Reflections and Future Issues.....	48
8 Bibliography.....	52
9 Glossary of Terms.....	59
10 Appendices.....	61
10.1 Research Assistance Request Letter.....	61
10.1.1 Employers.....	61

10.1.2 Recruiters.....	62
10.2 Student Research Conference.....	63
10.2.1 Abstract.....	63
10.2.2 Poster.....	64
10.2.3 Handout.....	65

Table of Figures

Figure 2.1 - Web 2.0 Mind Map (Angermeier, 2005).....	11
Figure 2.2 – Growth of the internet in the first ten years (Hinchcliffe, 2006).....	12

1 Introduction

“When it comes to gossip and rumor [sic] on the Internet... the culprit is ourselves. We're invading each other's privacy, and we're also even invading our own privacy by exposures of information we later come to regret.”

(Solove, 2007, preface vii)

1.1 Background

This project was inspired by a workshop held by Linda Jones, Law and Criminology faculty librarian at the University of Portsmouth, in May 2008. The workshop was entitled “The Darker Side of the Web” and covered topics such as copyright issues, identity theft and social networking amongst others. Further personal research into the subject indicated that increasingly more employers in the UK were using the internet to gain 'added value' information on potential employees. Data added by internet users, using functionality only recently provided with the inception of Web 2.0, can leave a trail of their activity for any interested party, including potential employers, to find using a simple search tool. The author found little UK oriented research into digital footprints and employability. This topic therefore offered scope for an interesting project covering relatively virgin ground.

There is growing evidence (Öqvist, 2009, p1-3) that governments in many countries are facilitating the storage of internet data by ever increasing, and expanding, legislation. Whilst this is being undertaken in the name of anti-terrorism and immigration control, much of this data may concern individuals not actively involved in either area. This data may be combined and aggregated with other digital sources, such as CCTV and biometric passports, to form a “virtual shadow” (Öqvist, 2009, preface xviii): an expanding online digital identity that we may know little of, but that follows us everywhere (Ibid.). It is the information our virtual shadows contain that may be used, misused, or lost by government or their agencies, or which potential employers may access during their recruitment process. This document will use the term “virtual shadow” (which is interchangeable with “digital shadow”) to represent this ever growing pool of digitally stored personal information.

The overall aim of this report is to make the reader aware of how past interaction with Web 2.0 functionality and applications may have some future use by employers, the state, and other interested parties. It is important that job seekers realise that they may not be invited to interview for some positions because of information held in the public domain. In addition to this, changes to government policy which could lead us towards a surveillance society of Orwellian proportions will be explored. Finally, it will discuss whether employers and further education establishments should publicise the potential loss of privacy associated with the individual's use of Web 2.0 functionality, and its impact on employability. For more novice users of the internet, the project also provides background information on Web 2.0 applications and the next generation of the internet, as well as details on the law relating to privacy and data protection, to illustrate the context in which such activities may take place.

To further these aims, the report will use a combination of primary and secondary research sources. These will aim to explore available literature on each element of the overall subject; that of technology used, and employer and/or state use of personal internet data, followed thereafter by a discursive review of the findings. The secondary research element took the form of a review of news, magazine and industry journal articles, and of the results of prior academic research, to identify how employers and recruitment agencies utilise personal information, not part of a candidate's CV or formal application. From these findings examples of the type of problems a candidate may encounter as a result of such activities are discussed. In addition to this, comment on personal and corporate preference relating to the subject of this project, was gained from an employer attending the 2009 student project conference in the School of Computing. As this project is related to both personal and professional internet use, many of the associated references were gained from online sources, and include references to online versions of printed journals and other academic texts.

This project will therefore answer a number of questions, as shown in section 1.2, using primary and secondary research sources. It is intended to make the reader aware of how data collected through past interaction with the internet, and changes to government policy could have some future use by potential

employers. It is important that web users understand that they may not be invited to a particular interview because of information held in the public domain.

1.2 Research Questions

With the project being entitled “Digital Footprints and Employability: A critical examination of the implications of digital identity with reference to the growing state and corporate use of data regarding employees”, a certain number of questions must be answered to assist the reader with their understanding of the subject area. As the subject of privacy is regularly discussed in the press and other publications, this project will have a cut off date of 31st March 2009 and therefore will make no comment on any article published after this date.

1.2.1 What Is Web 2.0 And Why Is It So Important?

This question will be answered through a literary review of available historical evidence. It will provide the reader with background information required to understand how ‘digital footprints’ are created, and the medium in which these footprints are left.

1.2.2 What Is A Digital Footprint?

An expansion of the initial literary review will provide background data defining the term ‘digital footprint’, and detailing its expanding use in both academic and non-academic texts.

1.2.3 What Is A Virtual Shadow And How Is This Relevant To Workplace Surveillance?

This will involve defining the term ‘virtual shadow’, comparing it to ‘digital footprints’, and relating this to employee surveillance.

1.2.4 Is There Evidence That Prospective Employers And Recruitment Agencies Utilise The Internet For Background Checks On Applicants During Any Recruitment Process?

In order to answer this question, primary research will be conducted asking a number of employers and recruitment agencies for their experience of internet

use during the recruitment process. To back up this data a further literary review will be conducted providing further examples.

1.2.5 Can Some Employee Interaction With Web 2.0 Applications Be Beneficial To Business?

Many employers are now introducing the usage of Web 2.0 style applications for business purposes. A review of some of these will provide the reader with examples including their perceived benefit to the business.

1.2.6 What Personal Data Is Stored And Potentially Used By The State Within The UK And Globally With Regard To The Workplace?

With the expansion of government agencies into the online world, it is important for internet users to understand what data is being stored, and its current and potential usage. A review of some online government applications relating to employment and employability, along with guidance within the law, will give a clearer understanding of any implications.

2 Web 2.0 And Digital Footprints

This chapter will perform a review of available literature, from both primary and secondary research sources, to describe the history and future of the technologies which are encompassed by the term 'Web 2.0', and introduce the reader to some of this terms uses and characteristics. The new phenomenon of digital footprints and virtual shadows will be defined and clarified. This will ensure that readers have an understanding of how general internet activity, specifically within Web 2.0 applications, can leave a trail of personal information that the subject may not wish to be taken out of context.

2.1 What Is Web 2.0?

Named during a conference brainstorming session attended by O'Reilly Media and MediaLive International, Web 2.0 as a concept came from the "bursting of the dot-com bubble" towards the end of 2001, when the internet progressed from simply being an online library of news and information into what can be seen today. There is some disagreement over the actual meaning of the term with perhaps a little over-usage by marketing companies, but Tim O'Reilly describes it as being a 'platform', a core of principles and practices that connect an extensive 'solar system' of similar sites, each a different distance from the core in terms of their conformance to these principles. Whether web sites and applications should be considered 'Web 2.0' is dependent on how many of the core competencies are demonstrated (O'Reilly, 2005, p1). The mind map shown in figure 2.1 overleaf "summarises the key aspects of Web 2.0 in a visual way using colour and text size to indicate importance" (Angermeier, 2005).

an article written in 1996, 8 years before O'Reilly's initial Web 2.0 conference, Berners-Lee described the future of the WWW as developing an "increasingly interactive nature of the interface to the user" and using "defined semantics" (Berners-Lee, 1996). This article shows us that whilst Web 2.0 as terminology provides a definition as to the more recent changes in how the internet is utilised, its original designer included these features in his original outline although the technology was not yet available to bring it to fruition.

A recurring view expressed by researchers in the area is that the major changes in the first 10 years of the internet could be classified as social change, rather than technological. As more people gain access to the internet, and there are now over 1 billion users, so we see new applications being created to cater for their needs. Dion Hinchcliffe of Social Computing Magazine (2006) noted that some of the companies working to create the next generation of the internet around the turn of the 21st century found it hard to encourage users to interact with the first forms of Web 2.0, software due to their worries about their lack of technical knowledge, and security concerns. The dramatic change in the use of the internet over its first ten years is illustrated in figure 2.2 below.

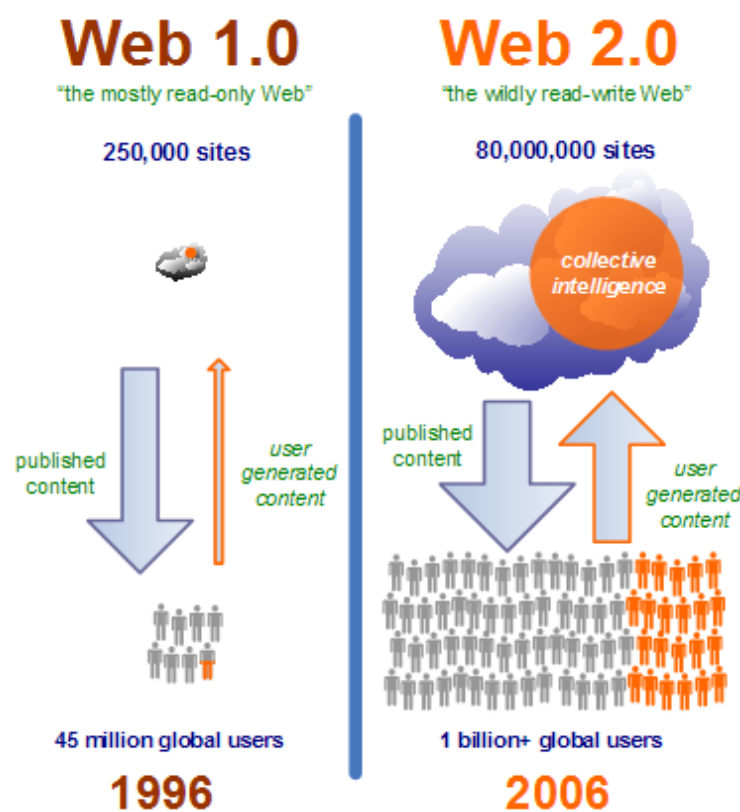


Figure 2.2 – Growth of the internet in the first ten years (Hinchcliffe, 2006)

One example of how the internet started to move from the more Web 1.0 characteristics of its infancy to those of Web 2.0 is in the connection of people via networked gaming software, for example multi-user domains (MUD's). Through simple code entered via the command interface on early computers, gamers were able to connect to another computer holding the required software to join a shared or 'networked' electronic game. Games were mostly command line based and required users to type phrases such as "say" and "whisper" to contact others and, although in their early days were mostly textual, some incorporated simple graphical representations of gamers and their surroundings (Turkle, 1995). This may represent the earliest example of internet user online identity selection, with corresponding opportunities to hide "meatspace" (Gibson, 1984), or real life characteristics from other online users. It became possible, via the internet, to exist in a parallel world free of the ties that bind us to reality, and to lose oneself, in a similar way to losing oneself in a good book. Of course, this was also the first time users started to leave digital footprints showing their progress through the internet along with details of their digital personalities.

2.2 Digital Footprints And Virtual Shadows

"Did you know that everything that you do online and offline [sic], if digitally stored somewhere and linked to your PII [personally identifiable information], becomes a part of your virtual shadow? Your virtual shadow is the accumulation of digital footprints that you leave behind." (Öqvist, 2009, p118)

When discussing the amount of data stored and accessed via the internet relating to personally identifiable information, two of the more used phrases include digital footprints and virtual shadows. There are various definitions of these terms, but for the purposes of this project a digital footprint is the trail of information personally left during regular internet usage and/or interaction with Web 2.0 applications. A virtual shadow is an expansion of this and covers the contents of your digital footprints, as well as comments made by others about you, "ambient" background information such as government or medical records, digital CCTV images, and travel details where a passport or other form of identification has been used (Gantz et al, 2008). Certain internet users may not wish their virtual shadow, or its individual digital footprints, to be viewed by others for any reason

as it could be taken out of context, or provide a view of a part of their personality they wish to only share with close friends. However, an individual virtual shadow may have no detrimental effect on its owner; in some cases they can provide proof of a well-formed character including activities undertaken for the benefit of others.

2.3 Web 2.0 Applications

There are many forms of technologies and applications associated with Web 2.0. This includes some that simply combine other technologies for new usage and others that have become applications in their own right (Pilgrim, 2008). Web 2.0 applications are created to use dynamic content most of which is provided by the users, and can come from many sources but be seen on a single page. This can include the syndication of news alongside user comment, the creation of shared web links or bookmarks, open source software with development shared by interested users, and topical personal social data (Lewis, 2006). Toffler discusses “the rise of the prosumer” (1981, p275-299), referring to the blurring of the roles of producer and consumer, beginning with the introduction of the “do-it-yourself pregnancy test kit”. This has moved on to a point where applications associated with Web 2.0 would normally have some or all of their content provided by the very people consuming the output. This section will consider, explain and explore some of the more heavily used terms associated with Web 2.0.

2.3.1 *Social Networking*

Of the top ten websites listed by average page access data over a three month period on Alexa.com, a database providing internet statistics, (“Global Top Sites”, 2008), two are classified as sites used predominantly for social networking. At number 5 is Facebook with approximately 12.5% of global internet users visiting it on December 4th, 2008 and MySpace is at number 7 with 5.41%. These numbers may not sound very large but together they show that almost a fifth of all internet traffic is directed at just two of the many social networking sites in existence. Social networking sites have varying uses matched by the different social groupings which regularly use them. Some, like Bebo, are aimed at pre-teenage children, whereas others have been created to provide a focal point for those

interested in such things as Gothic culture, business, books, particular religions, and dating or relationship advice for adults. One of the lesser known websites, Ning, allows users to create and customise their own social network (“List of Social Networking websites”, 2008).

Facebook was created in February 2004 by students at Harvard University and before the end of that year had almost 1 million users. Initially it was only available for use by Harvard students, but was so popular it quickly expanded to other major US university campuses and those with a .edu e-mail address. It claims to currently have “more than 130 million active users” and “over 55,000 ... networks”. The site allows registered users to upload personal information (e.g. likes and dislikes, phone numbers, photos) as well as create or join special interest groups, post items such as videos that may be of interest to those in their personal network (named as ‘friends’) and invite others to events. Those who users invite to be ‘friends’, after accepting the initial invitation, are provided with updates on their activities and current status as well as having the ability to interact with other profiles by leaving short messages on the “wall” (Facebook, 2008).

In addition to interacting with ‘friends’ users can download small applications, not all of which are stored on the Facebook servers, to enhance their interactions. These applications include those specific to gaming, music, dating, travel and sports amongst others. Using a form of viral marketing, or the spreading of knowledge regarding these applications by word of mouth, these are collected by users who pass them to others in their network of friends. Three applications, which included two games, were created only for research purposes and generated millions of pages of internet traffic. These were, in total, used by more than 7 million unique Facebook users (Nazir et al, 2008). There are those who create applications not to show their development prowess, but to steal personal information from the many users. Sophos, one of the more respected providers of security software, conducted research into how many users would be willing to freely give away personal information by accepting a friendship request from a small plastic frog called ‘Freddi Staur’ “an anagram of ID fraudster” (Sophos, 2007). Out of the 200 randomly selected users 87 accepted the request to be friends and 82 of these divulged personal information such as e-mail addresses,

date of birth, home address and phone number (Ibid.). This simple experiment proves that many users of social networking sites are naïve when it comes to protecting their personal data over the internet. “Each time we post something on the web, our 'footprint' gets bigger” (Kelly, 2008); we are constantly adding to our digital footprints and often do not realise how this information, freely given, can be used by others with criminal intent or by employers to gauge our personality types.

2.3.2 Blogging

In December 1997 “Jorn Barger, author of the site Robot Wisdom, created the expression “weblogs” to describe what he and several other internet pioneers are doing on their sites” (“A brief history of Web 2.0”, n.d.). The term ‘weblogs’ was soon shortened to the phrase we know today as a simply ‘blog’ or ‘blogging’. They have been likened to online diaries and allow people to express their opinions on a myriad of subjects on many different websites. Users can communicate to others their thoughts without fear of mediation, and are at the same time open to others commenting on their work with the same openness. Posts can contain simple text or can be enhanced by the use of images, links and other relevant items. Some sites in the ‘blogosphere’ (a name given to the ‘universe’ of blog sites) are specifically created to provide one persons opinion; others, similar to social networking sites, allow registered users to create their own and comment on others individual blogs (Agarwal, 2008). There is also a term used to define web pages providing a list of links to other blogs that may be of interest to the reader – blogroll. The growing use of the internet by individuals to publish their own work, thoughts and ideas lead The Times newspaper to give their annual ‘person of the year’ accolade in 2006 to “You” (Ibid.).

2.3.3 Wiki's

Wiki is a word taken from the native language of Hawaii and means quick or fast (“Glossary of technologies...”, n.d.). To better understand the nature of a wiki it is probably useful to refer to the most successful of these, Wikipedia, which is the eighth most used website globally (“Global Top Sites”, 2008). It is thought that the first reference to a system similar to what is currently termed as a ‘wiki’ was written by Vannevar Bush in 1945 when discussing the Memex, a device to assist

researchers with locating information stored on microfilm by using notes and associated links left by other researchers. The creation of the internet brought with it the idea of better collaboration between developers and led to the development of the first web based wiki by Ward Cunningham in 1995. The WikiWikiWeb was originally designed as an experiment but proved itself to be so popular amongst developers that other “wiki clones” were soon developed. The first to be introduced for public use was Wikipedia launched in 2001 as a “free content encyclopaedia” (“History of Wikis”, 2008). All entries are provided by registered users with a request that they cite their sources for others to follow. Wikipedia has a reputation for being a poor source for researchers as there have been instances of deliberate misrepresentation, and unreferenced and/or unproven information being added to the site. With such a large user membership however, deliberate attempts to undermine the power of the site are normally corrected within a short time frame (“Wikipedia”, 2008). Its very inclusion in this report proved to be hard decision; however the author concluded that the references used to provide evidence for this dissertation provided sufficient citations, and that it would be difficult to evidence the use of wiki’s on the internet without mention of its greatest success.

One of the more recent uses for wiki technology has been in the field of teaching and learning where students are taught the value of collaboration. However, there is still an element of apathy from the students themselves in adding and editing entries. This could be caused by the student having no confidence in their own work and thought, but blame can also be placed at the overall design of the wiki (Cole, 2009) making users uncomfortable with its use.

2.4 The Future And Web 3.0

Tim Berners-Lee saw the third phase of the internet “allow[ing] the web ... to contain rich data in a form understandable by machines, thus allowing machines to take a stronger part in analyzing the web, and solving problems for us” (Berners-Lee, 1996). There is however dissent or refusal by some commentators to accept this as the true definition of what is yet to come. There are theories that the web will be more than could have been thought of originally and could include elements of three dimensional or VR access. One idea, the pervasive web, incorporates internet access within many alternative formats

including “web connected bathroom mirrors” and windows that know when to open and close based on the local weather forecast and current conditions (Metz, 2007). A system such as this could provide the ultimate in updatable information; users would be able to refer to current weather conditions uploaded automatically to the internet by their own homes. The “intelligent home” has already been reported in the press (Cope, 2000) but could include a refrigerator that would define its own shopping list by wirelessly communicating with other food storage areas, and ordering it to be delivered at a convenient time located in an online diary. Berners-Lee saw the ultimate development being the semantic web, which would utilise additional metadata (data about data) to assist with the organisation of our schedules as an example. We would be able to look at internet data based on its meaning, linking information based on similarities. An article appearing in Scientific American co-authored by Berners-Lee described a process where a fictitious person could automatically link a doctor’s prescribed treatment to local providers which are covered in a particular health insurance plan, along with a convenient time in their personal calendar. All this could be completed with one simple semantic web search (Metz, 2007). With the internet itself being a relatively recent invention, and the speed at which it has already transformed itself into its current state, it cannot be long until we move onto the next phase, but what form that will take is still to be decided.

2.5 Chapter Summary

- Web 2.0 represents the changing trend in use of internet technologies to include more interaction and more user content.
- The consumer-creator economy and the creation of larger personal digital footprints can be useful to recruitment agencies and employers.
- Tim Berners-Lee envisaged the coming changes to the internet from its beginnings through to the semantic web in 1996.
- The internet grew from an initial 45 million users globally to over 1 billion within 10 years.
- Web 2.0 applications account for a large percentage of overall internet traffic.
- The future of the internet could bring 3D or virtual access, but will include semantic elements.

3 Corporate Use Of Personal Internet Data

Following on from the previous chapter looking into current internet technologies, this chapter aims to review available literature and describe how information placed into the public domain via the internet, perhaps using applications such as those discussed in chapter 2, could be utilised by potential and current employers, and is further discussed in section 6.1. Such data may be entered personally through the use of an unsecured social network profile, blog or wiki entries, or could be entered by friends or acquaintances without your knowledge.

3.1 Generation Google

The recent growth in the number of individuals using Web 2.0 technologies to provide them with an online presence has been described by researchers as the beginning of “Generation Google” (Solove, 2008, p9). This follows on from the previous Generation X and Y cohorts discussed during the mid to late 20th century (Ibid). Google is an internet site that searches for web pages containing pertinent information based on user supplied search criteria, listing and ranking these pages by order of relevance. In the ten years since its creation, Google.com, the main US and global version of the website, has reached number 2 in the Alexa traffic rankings. The top 25 globally ranked list contains six versions of the Google search engine including those from India, UK, and Germany (“Global Top Sites”, 2009). More recently, especially with the introduction of further enhanced Web 2.0 applications, it has proven easier to find differing types of information on a person or company simply by performing a web search. “People google [*sic*] friends, dates, potential employees, long-lost relatives, and anybody else who happens to arouse their curiosity” (Solove, 2008, p9). Indeed, the colloquial term “Googleability” is used to describe “[t]he ease with which information about a person can be found on an internet search engine, particularly Google” (McFedries, 2007). As examined in this chapter, there is evidence that these searches are performed by potential employers looking to gain a better understanding of their applicants, or current employers wishing to observe their employees’ online activity for any potential misdemeanours.

It is not just use of generic search engines, such as Google, that could have a detrimental effect on your online reputation. Other, more specifically created

'people' search engines such as Pipl, Spock or ZoomInfo have been developed to read information from many websites, including social networks, to provide an additional 'personal profile'. Although these profiles may not necessarily directly relate to the originally searched person, as others may have the same or similar name, anyone who has a presence in one or more Web 2.0 style applications is more likely to be found (Tynan, 2008). At present, these people search tools are mostly aimed at the American market, but it cannot be long until these, and others, become populated with UK content. It is imperative therefore, that those of us who take an avid interest in their personal online reputation for whatever reason, should regularly perform these web searches to ensure they are not the victim of spoof profiles, or the subject of another's online tirade.

3.2 Dataveillance And The '24 Hour Employee'

"Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 2009). The term "dataveillance", first used by Roger Clark in a 1988 article for the ACM, covers both personal and mass scrutiny of collected data. He discusses this form of observation being used on an individual who may be of interest to a particular agency, such as those maintained by governments, or to an employer where there is suspicion of illegal activity or rule breaking (Clarke, 1988, p499). In more recent times, with the exponential change in data storage capacity, such data has become easier to accumulate. Employers have become interested not only in information gleaned from employee applications, but also their working practices and even how they spend their personal time (Joinson & Whitty, 2008, p39-40). It is this that has assisted in, and led to the use of the term "24 hour employee". This term can relate to employers who feel it is necessary for staff to constantly check their corporate e-mail and voicemail, even outside of working hours, but has also become a colloquial term for a constant watch on employees by management ("The 24-hour employee?", 1999).

Research undertaken last year in the United States showed that there is an almost universal storage of "employee's telephone records, internet activity and emails" within most large corporations (Joinson & Whitty, 2008, p39-40). Other investigations undertaken prior to April 2000 found that employees' use of the internet was under observation in over 70% of companies (Castells, 2001, p173).

In the UK the Regulation of Investigatory Powers Act (“RIPA”) was ratified in the year 2000 allowing the government and their investigatory and security services access to data when investigating possible crime or terrorist activity. Many people do not know however, that later additions to the Act also allowed “businesses to intercept communications in the course of lawful business practice without the express consent of either the sender or the recipient” (“Regulation of Investigatory Powers Act 2000”, 2006). This has caused some consternation amongst various official and charitable organisations, with the TUC (Trades Union Congress) demanding an official code of practice for employers (McCarthy, 2000) to curtail misuse of this aspect of the legislation.

3.3 Employee Recruitment And Internet Presence

Other new phrases to recently enter the English language are ‘cyber-vetting’ and ‘NetRep’. The former relates to the process used by some employers to gain further information on their employees, with the latter being the outcome of these searches; a persons internet reputation. If an employer ‘Googles’ an applicant during the recruitment process, what they find could give an additional picture of the applicant (Paton, 2007). The formal application and CV of a prospective employee may be outwardly professional and particularly impressive, but comments, photographs, video, both posted by the individual or by others and relating to the individual, and openly available through their social networking site of choice, may expose elements of their life to the employer which paint a very different picture. In addition, potential employers may find personal blog entries relating to current or previous employers which may contain derogatory and possibly inflammatory entries, and which may reflect badly on the potential employee. Collectively, the information which may be found about an individual via searches on the internet by a potential employer or recruiter goes to make up that individuals internet reputation (NetRep). A client study undertaken in March 2007 by the UK based recruitment agency Poolia showed that two thirds of the 500 employers polled “admitted regularly carrying out internet searches, including checking social networking sites such as MySpace, Facebook and YouTube” (Paton, 2007). On a more positive side, it is possible that employers may see some of your online entries as a sign of a balanced and happy personality.

Whilst online research provides many examples of organisations utilising the internet to gain further information on applicants, very few of these will formally admit that it is part of their standard process. “It’s essentially information many corporations shouldn’t be looking at” (“Online Social Networking...”, 2008). UK based recruitment companies Crone Corkill and FSS surveyed their joint client base in 2007 demonstrating that, at the time of the study, 7.5% of UK corporations were actively using social networking websites for ‘added value’ information on applicants. This activity, with the introduction of specific ‘people’ search applications and enhancements to Google, is now expected to be effortless and therefore more highly used (“Employers turn to Facebook”, 2007). There are a limited number of online networking tools which have been created specifically for business use, for example LinkedIn.com (see section 3.6), which specifically provide “testimonials for a candidates [sic] professional background – which would actually enhance and not damage reputation” (Ceridan, 2007).

3.4 Examples Of Employment Problems Associated With Internet Presence

The internet, along with journalistic and academic publications, provide varied examples of where internet use has led to an employee’s dismissal, or to an applicant not being offered an interview for an advertised post. One such example involves an Irish banking employee who informed his employer that he had learned of a family emergency, thus requesting some time away from the office. Subsequently, their employer found, on Facebook, photographs of the staff member, taken during their period of leave, attending a fancy dress party in America. Needless to say, this did not appear to constitute a normal family emergency, and therefore they were dismissed (Kennedy, 2008).

One quite infamous story of employees being asked to leave a company because of comment made online, involved thirteen cabin staff working for Virgin Airlines. A Facebook group was created where staff discussed the safety and overall cleanliness of the aircraft, also quite openly referring to customers as “chavs” (Conway, 2008). Virgin, dealing directly with the Facebook administrators, requested that the group be closed, commenting that there were better channels in which staff could air their views. The same article published on the Independent Newspaper website in November 2008, refers to other similar

stories. One told of a man who lost his job at a Waitrose store in London when a colleague presented copies of derogatory online comments regarding the company to his employer, and another spoke of a man being fired from a well known catalogue for creating a group called “I work at Argos and can’t wait to leave because it’s shit [*sic*]” (Ibid.). These people did not appear to consider that what they had placed online may have been found by their employer or colleagues, and that there may have subsequently been detrimental consequence.

A HR director working for a financial services company in Canada noted a particular experience where the company were in the process of making an offer to what they considered to be an exceptional candidate. The director decided to take one last look at the more personal aspects of the applicant, and an internet search provided them access to the candidate’s MySpace page. The candidate had made no effort to disguise their use of recreational drugs, and the organisation considered that this may, at some point in the future, have a detrimental effect on their corporate image. As a result they made the decision not to make the offer of employment (“How social networking sites...”, 2007).

Students must now be aware that they may be the subject of some form of ‘cyber-vetting’ when seeking their first post graduate role, although not all students may take part in or openly publicise online activities such as those discussed above. Corporate use of internet data regarding individuals and its potential impact on job seekers is discussed further in section 6.1.

3.5 Personal Internet Use At Work

As discussed earlier in this chapter, “employee surveillance is near ubiquitous” (Joinson & Whitty, 2008, p39). To ensure they are acting within the law, organisations are now providing their staff with copies of acceptable use policies (AUP’s). These documents contain details not only of the expected behaviour of any employee with regard to their use of business technology, but also the consequences of misusing this privilege. AUP’s can be enforced with the use of e-mail filters for both incoming and outgoing messages, and tools that can either block or restrict employee access to certain websites through the corporate network. “The electrical retailer, Comet, which normally operates ... a “culture of

trust"...has taken the decision to ban staff access to Facebook" (Naylor, 2007, p3). UK Acts of Parliament, such as Regulation of Investigatory Powers Act, 2000 (RIPA) and the Data Protection Act, 1998 (DPA) (see section 4.2), have given employers the legal right to use surveillance techniques to monitor their employees providing there is some reasonable cause, and they have made employees aware of the corporate policies (Naylor, 2008, p4). As further discussed in section 6.1, it is not necessarily just the potential loss of working time that internet use may result in that concerns employers, but also the potential risks of loss of confidential data, or of employee downloading of illegal content, or posting content slighting their employers onto social networking or blog sites.

Future developments in computer use and personal surveillance may include the remote monitoring of physical processes, which change in reaction to external and internal stimuli, and over which we have no control. If a US Patent application by the Microsoft Corporation is approved, technology will be available for interested parties, such as employers, "to monitor employees' performance by measuring their heart rate, body temperature, movement, facial expression and blood pressure" (Mostrous & Brown, 2008). The original idea behind the technology was to provide data showing the frustration and stress levels of employees during any given day. The data could then be used to predict whether some intervention was required thus preventing any permanent physical or mental health damage. Commentators considered this invasion of personal privacy to be a step too far, and noted that this technology could be used to monitor employees at any time, not just during standard working hours (Ibid.). If this patent were to be approved and the technology created to manage this, it may not be long until these surveillance techniques are added into corporate AUP's thus becoming almost second nature in the workplace. How many of us would want employers to know about personal issues, or that you may be finding a particular element of a set task difficult. It is these very difficulties that can make us stronger people and therefore better employees. For some, the very fact that they were being monitored could raise their stress levels even if they were coping well in both their work and personal lives.

3.6 Social Networking For Business

As further discussed in section 6.1, employees in the digital age are more likely to want to use some form of networking tool both inside and outside of working hours. Collaborative working tools, linked to task or project management software, can provide staff with a simple way of updating and disseminating information regarding their current status, sharing documentation, and leaving a persistent record of change over time. Other options include the provision of simple forums allowing staff to ask questions of each other. Whilst people working in your immediate location may not be able to provide an answer, there may be those in other offices who could assist. It is highly important that these tools are linked in with corporate AUP's and managed effectively ("Bosses 'should embrace Facebook'", 2008).

Some companies are active in their use of social networking tools to enhance their business. The British Computer Society (BCS) has its own page on Facebook allowing users to become 'fans', receive updates on upcoming lectures, contact other users, and use the discussion boards to provide their own comment ("The British Computer Society", n.d.). Other businesses have created profiles on Facebook to allow employees past and present to stay in touch with one another ("Can social networking expand...", 2008). Ernst & Young, the global financial company, has a profile specifically created to enhance their recruitment process, providing interested users with a direct link to the company, as well as marketing tools such as a question and answer section ("Ernst & Young Careers", n.d.).

Newer, and more business oriented, social networking tools such as ZeroDegrees and LinkedIn allow those working at a more senior level, along with others who may be working for themselves, to connect through online introductions from known contacts. LinkedIn allows users to 'recommend' contacts, and these can be viewed by any person viewing your profile. Working in a similar way to an extended CV, users can add details of previous employers with details of their responsibilities. The design of the website allows anyone to view your details, but provides updates to inform you of how many others have viewed your profile, and which industry they are from. Through their introduction system, business users can be introduced to potential clients and collaborative

partners, as well as use the site to discuss issues particular to their field of interest and search for new job opportunities (LinkedIn, 2008). Whereas previously senior executives and sales people would have relied on privately stored “black books ... and rolodexes”, they can now share details of their contacts easily with others making the process of collaborative working and business networking easier (Boyd, cited in Jardin, 2009).

3.7 Chapter Summary

- Specifically created ‘people’ search engines along with Google are being increasingly used by recruiters to gain an ‘added-value’ insight into applicants.
- Large corporations are storing more employee telephone, internet activity and email details due to the growth in data storage capacity.
- A mismanaged internet reputation (NetRep) can have an unforeseen effect on job applications.
- Two thirds of UK employers polled in a 2007 survey admitted to searches of social network sites during the recruitment process.
- Making derogatory comments about current and previous employers online could lead to dismissal and/or problems with future employment.
- Students and graduates need to ensure they have a consistent online profile that they would be happy for an employer to view.
- Some online networking tools can be beneficial for business.

4 The Law, The Government And Corporate Access To State Data

Following on from the previous chapter which discussed corporate use of personal internet data, this section will consider different types of online applications used by government agencies for the collection, dissemination and storage of personal internet data with regards to employment and employability. This includes requests for access to data stored by government agencies from private corporations, and the law surrounding data access, and these findings are further discussed in section 6.2.

4.1 E-Government

In April 2004 the UK government launched the online DirectGov portal, with the aim that it would be complimentary to the many other local government sites. The portal offers users a single point of access for information regarding government services, along with links to specific tools including online payment systems for Council and Car Taxation (“DirectGov demonstrates...”, 2005). This centralisation of personal data, including details of benefit payments and disabilities, could be viewed not only as a major security risk but also an invasion of privacy. It is difficult to guarantee how many people might have access to your personal data, and how this information may be shared across departments.

“Gordon Brown is being reported as having said that some data loss from government is inevitable because one cannot eliminate human error” (Evans, 2008). If data is being lost by government agencies, would it not be as easy for someone with criminal intent to steal or amend personal data? Individuals could be, whether intentionally or accidentally, added to databases preventing them applying for employment requiring contact with children or vulnerable adults. In 2008 the British Computer Society (BCS) reported how a new computer virus called Asprox was found to be on both health service and local government websites, and “is now present on two million computers” (“Government sites...”, 2008). The code allowed the hacker to retrieve details, such as bank account data, directly from a user’s PC; proof of the ease with which data can be stolen.

4.1.1 Data Snooping

In October of 2008 the home secretary, Jacqui Smith, confirmed that the government were considering a proposal which would allow the security and intelligence services access to personal internet data, including information from a wide array of sites including social networks. The access would allow the monitoring of individuals for any criminal or terrorist activity undertaken using pseudonyms. Currently, the only data available to these agencies is provided by communication service providers (CSP's) and consists of nothing more than billing records; other access, such as the ability to listen into telephone conversations, requires a ministerial warrant. Whilst Ms Smith confirmed that their interest lay more in ascertaining the location of a suspect than the content of any conversation, there are still those in parliament nervous of a propensity towards mass dataveillance (see section 3.2 for clarification) (Norton-Taylor, 2008). Data gathered in this way could be used alongside other methods of tracking, such as the ability to track commuters in and around London using 'smart' cards such as the Oyster card which provides an electronic, contactless means of payment for public transport in the London area, to profile individuals (Hinsliff, 2008).

Employers such as government agencies, the armed forces, and certain private sector service providers, require staff to gain necessary security clearances prior to commencement of employment. These checks are undertaken as requested by the Defence Vetting Agency (DVA) and any suspicion of illegal activity could delay clearance, or in some cases cause this clearance to be refused. The employer will not be provided with details as to the cause of the delay or refusal, as any information transfer could be considered in breach of the data protection act ("What is security clearance?", n.d.). The author gained personal experience of this security clearance procedure whilst working for the National Air Traffic Service (NATS) in the summer of 2007. Staff not directly working within any of the operational air traffic control units, could be provided with a security waiver covering the lack of clearance until formal confirmation was received. Although permanent UK citizen status was established, and with a contract of employment lasting just four months, the authors' final clearance was not gained until two weeks before contract completion. This delay was apparently normal and anecdotal evidence provided at the time attested that some employees were still

awaiting final clearance up to, and in excess of, 5 years after commencing employment. Whilst not directly related to data snooping, this evidences another process where government agencies have legal access to your personal data. As employers and employees are often not informed as to the specific nature of any delay or refusal, they have little or no opportunity to clarify or correct any potential errors in personal data. In addition to this, the fact that some employees are able to commence employment in secure areas under a security waiver, authorised by the line manager, leads to the question of need; if employees can be recruited prior to clearance being gained, is the clearance truly required?

4.1.2 National Databases

The many varied UK government departments hold a plethora of information on citizens within their individual databases. These include:

- **National Identity Register:** Linked to the introduction of ID cards, it holds data on your name, address, gender, date and place of birth and may hold biometric information such as fingerprints and iris patterns.
- **Criminal Records Bureau:** Contains name, address and details of any person convicted for criminal offences.
- **Passport database:** Contains your address, date and place of birth and your travel history.
- **UK DNA database:** Largest DNA database in the world covers 5.2 per cent of population with 30,000 additions every month. (Verkaik, 2007)

Of those listed, the most disturbing could be the exponential growth of the UK DNA database. Since 2004 this database has included any person who may have been arrested without charge, as well as acquitted drunk drivers. Out of over 4.2 million profiles stored, “700,000 belong to children and 30 of them are under 10 years old” (Privacy International, 2006b cited in Öqvist, 2009, p137-9). The further addition of profiles belonging to citizens who have officially committed no crime has been contentious; this includes the addition of information concerning minors. “It is expected that nearly 1.5 million 10-18 year olds will have been entered on the national DNA database by Spring 2009” (Öqvist, 2009, p139). Whilst it may be that the database should only be seen as a force for

good, the longevity of the information stored should also be taken into consideration. In some countries, such as Sweden, DNA profiles have been used to provide identification of disaster victims. This has led to a proposal being considered in the UK to add profiles to the database without consent (Ibid., p139-41). The possible future ramifications of this continued storage of DNA profiles is further discussed in section 6.2.

In 2004, the UK Passport Service (UKPS) were considering introducing a linked database with that of the newly created National Identity Register (NID). Once complete, this merged database would contain more detailed information on individuals. The addition of biometric information with passports, such as fingerprints and iris scans, means that these documents, whilst allowing for easier travel around Europe and the rest of the world, hold a large amount of personal information (Nash & Arnott, 2004). Five years after this original disclosure the work to create the centralised database has almost been completed; any application for a UK passport made from 2009 onwards will automatically qualify you for an ID card. Any person refusing to allow their personal details to be held on the new database will also be refused a UK passport therefore preventing them any international travel; however citizens do not necessarily have to accept the card itself (Slack, 2007). If at some point in the future this enhanced NID information were to be added to the DNA and growing medical records databases, anyone with access could discriminate in ways shown below and further discussed in section 6.2. This database would be easily accessible when required, but will also record when elements of your record have been read and by whom. It could lead to the 'profiling' of citizens who may find others interested in how their lives are led on a daily basis; this could include benefit payments, mortgage applications, requests for security vetting and even the outcome of medical checks. Whilst there are very few people currently on the database, many more are being added daily with applications for new or updated passports, or as part of the immigration process (Boggan, 2007).

Finally, the UK government has, since February 2008, been centrally storing personal details of every 14 year old English child along with the results of any examinations. Each child has been provided with a 'learner number' which is at

present discarded once the child has left school. If a new database proposed by the Learning and Skills Council (LSC) is constructed, this number will allow for a record of all education to be stored. The aim would be for this 'electronic CV' to be tamper proof by the individual, thereby allowing employers and further education establishments a trustworthy level on which to test the academic details of any application (Öqvist, 2009, p126-7). Anecdotal evidence suggests that, if polled, potentially many employees would admit to a small amount of embellishment on their CV when applying for posts. However if detailed academic records could be easily checked by employers, more emphasis could be placed on employment history. As Lee McQueen, the winner of BBC1's The Apprentice programme found in 2008, it is not always easy to hide your background. His application claimed he attended university for 2 years, but some confusion over the dates on his original CV led to him admitting to no more than 4 months (Woods, 2008).

A recently published report commissioned by the Joseph Rowntree Reform Trust Ltd. reviewed details of a number of government databases, and commented that "in too many cases, the public are neither served nor protected by the increasingly complex and intrusive holdings of personal information invading every aspect of our lives" ("Database state", 2009, p4). Possibly the most important finding of this report was that approximately 25% of these databases are in breach of current data protection laws, and also infringe our human rights. These databases include some already mentioned in this report such as the DNA database and the National Identity Register ("Database state", 2009, p5). One database in particular, ONSET, could have a serious bearing on an individual's future employability. This system, created by the Home Office, attempts to "predict which children will offend in the future" (Ibid.) by interviewing them and their parents and comparing this information against other factors such as their environment, education, health and family history. Those at risk of offending are referred to youth support programmes and, should they require the assistance of the police, could find themselves being "treated as suspects rather than as victims or witnesses" ("Database state", 2009, p20). If this information were to be used at some point in the future as part of the vetting process for new teachers for instance, it could have a direct bearing on whether they are cleared and therefore offered a post.

4.2 Law Relating To Privacy And Identity

In the UK there are two main laws covering the protection and use of personal data. These are the Data Protection Act, 1998 (DPA) and the Regulation of Investigatory Powers Act, 2000 (RIPA).

4.2.1 *Data Protection Act, 1998*

On a basic level this law provides protection against the misuse of any personally identifiable data regarding an individual. Any person or organisation who may be using this data must act in accordance with what are known as the “Data Protection Principles” stated in Schedule 1 Part 1 of the Data Protection Act, 1998 (DPA) as follows:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In addition to the management of data, an individual has the right to request access to any paper and computer based records held in their name. Under this law every person has the right to request that information gathered is corrected

where necessary, and to prevent their details being used in marketing information. An important aspect of this law includes the right to prevent any decisions being made by an automated system where there is no human input (“Data Protection Act”, n.d.). There is no section of the law specifically covering the use of general internet searching by prospective employers as this information is held in the public domain; however automated searching could prove problematic at some point in the future if the government continues its process of merging individual databases. Errors in the initial data could eventually lead to the record of one person being mistakenly linked to that of another with similar details. Those applying for employment where security clearance is required may be denied the post based on an automated search of these merged databases. The exponential growth of data storage in every aspect of our lives requires each person to begin to take responsibility for their own data trail, or virtual shadow. With this in mind the Information Commissioners Office, a government agency specifically set up to “promote public access to official information”, has published a ‘Personal information toolkit’ on their website (“Personal Information toolkit”, 2007). This document should be read by any person interested in the storage or dissemination of any personal data stored by the state.

A proposed amendment to the Coroners and Justice Bill, known as Clause 152, if approved would give the government “an almost limitless range of data sharing opportunities both within government and between commercial organisations” (Privacy International, 2009, p4). These opportunities include, but are not exclusive to such things as:

- the transfer of medical records for research without consent
- further expansion of the DNA database for non-criminal related reasons
- service providers to provide all telecommunications data to the government in full
- national identity register to be populated with taxation and electoral role records
- the disclosure of prior academic records and family finance to monitor university entrance

Many of the proposals are in direct conflict with the current DPA law and therefore the changes have been moved into a further consultative stage (Privacy International, 2009, p4-7). The government public bill committee decided in March of 2009 to remove clause 152 from the bill on a temporary basis, and made a recommendation for further consultation (Public Bill Committee, 2009, col. 585). Chapter 6 of this report discusses this subject further and makes comment on how this could be of relevance to those seeking employment.

4.2.2 Regulation Of Investigatory Powers Act, 2000

Whereas the DPA regulates how personal information should be stored and protected, the newly created and updated Regulation of Investigatory Powers Act, 2000 (RIPA) allows for the surveillance of UK citizens including “access to electronic data protected by encryption or passwords” (Home Office, n.d.). RIPA was originally approved to ensure that surveillance was correctly regulated, and to set limits on the types and numbers of people and agencies who would be able to gain access to data. As an example, those working in the security services would have more access to private data and covert surveillance techniques, whereas on a more local level, authorities would only use the powers to assist, where required, on such things as benefit fraud (Home Office, n.d.).

The most contentious issue surrounding RIPA is the interception of “communications data” (“The RIP Act”, 2000). Whilst some commentators consider this to be a gross invasion of personal privacy, the UK government has replied confirming that only “clickstream” (Ibid.) (see glossary chapter 9 for clarification) data will be stored where required. Internet service providers (ISP) are required to store this clickstream information generated by their customers in a similar way to the lists of numbers called are stored by telephone companies. In addition to the interception of data, the security services can also request security keys for decoding encrypted data with a threat of incarceration for those who refuse (Ibid.).

For employers, RIPA allows for the capture of internet and e-mail usage through the organisations network as part of an agreed monitoring process (see section 3.2). Corporations also have to consider the danger that information requested

by members of the security services could be lost or stolen. The outcome of such a loss could lead to businesses losing confidential data relating to current business opportunities, and/or illegal access to confidential data using stolen encryption keys (“The RIP Act”, 2000).

4.3 Chapter Summary

- The UK Prime Minister considers government loss of personal data to be inevitable
- Under UK law the security services are allowed to access internet usage profiles of specific citizens.
- Incorrect data held by government agencies could lead to refusal of security clearance and therefore certain types of employment.
- State databases such as the UKPS and NID are being merged to provide more detailed profiles of UK citizens.
- The national DNA database contains profiles on innocent members of the public including children.
- The Learning and Skills Council database is considering storing details of all student academic records eventually leading to an electronic CV.

5 Fieldwork

5.1 Methodology

In order to investigate the original research questions associated with this project to their fullest extent, a combination of both primary and secondary research methods were required.

As mentioned in section 1.2, the subject of privacy is regularly discussed in the press and other publications. To ensure this project is published as per the University schedules, it will make no comment on any article or paper published after the date of 31st March 2009.

5.1.1 *Primary Research*

Letters were sent to twelve major employers and five employment agencies with offices located in Hampshire asking for details of their use of internet searches during their recruitment process. Where possible, following the initial contact, the author has planned to carry out confidential interviews with representatives of those organisations responding to the initial request to gain further information on internet based activities incorporated into the recruitment process, and which may be particular to the organisation. Copies of these letters have been included in appendix section 10.4. Other primary research, such as professional or academic field studies are to be utilised where possible.

5.2 Results

As discussed in section 3.3, there was an inherent risk that no person or corporation would reply to the original request for information as part of the primary research phase due to the informal nature of such online research activities. As predicted, no replies were received and therefore no specific results can be analysed.

5.3 Fieldwork Methodological Critique

The original letter initiating contact confirmed the acceptance of confidentiality, and that no mention would be made of specific companies or persons in the final report; however with the confidentiality associated with employee recruitment and

retention there was a risk that this project would fail to receive any direct comment. Whilst an element of primary research would have assisted in the validation of findings from secondary sources, this risk assumed the possibility that none of those contacted would feel able, either through personal choice or corporate guidelines, to provide any specific comment. With the specific timing involved in producing the final report it was not feasible to recruit any further participants, and again due to the issues raised above there is a likelihood that any further contacts made would still have declined to respond.

The lack of data related to the primary research phase does not necessarily prove that employers and employment agencies in the local area do, or do not, make use of the internet during any recruitment process. As was noted in section 3.3, professional research undertaken in March 2007 provided evidence that employers “admitted regularly carrying out internet searches” (Paton, 2007). In this instance the presumption can be made that it was decided, either at an individual or organisational level, not to provide any information either general or specific for addition into this particular study. Given that this is a sensitive area, the lack of response could indicate that this is widespread but that corporations treat it as an internal private matter, however this is purely speculation.

6 Discursive Review And Examination Of The Implications Of Digital Identity

As noted in section 2.1.1, users of the internet have been leaving digital footprints since the early use of networked gaming in the 1980's. In more recent times, internet use has become almost ubiquitous in the daily lives of many of us, yet still it seems apparent that a large number still have little understanding of the workings of the internet. These people may have never considered how the simplest of interactions could leave a trail of digital footprints leading to the creation of a personal virtual shadow (see section 2.2 for clarification). It is important therefore, that we recognise their existence and work to manage their impact on our overall digital reputation.

Whilst the current older generation, such as those over 50, may have comparatively only recently been introduced to the concept of computing both at home and at work, those under the age of 30 would have received an element of technical familiarization during their compulsory education. Marc Prensky (2001, p 1-6) examined the differences between these two groups and categorised them into two distinct groupings, digital immigrants and digital natives (see glossary chapter 9); those who were not born into the digital age and those who were. Many of these digital natives were introduced to Information and Communication Technology (ICT) as part of the national curriculum aged 5-7 years during the Key Stage 1 element of their education ("The National Curriculum...", n.d.) and often have a better understanding of technology than their parents. This however could lead to a certain amount of apathy amongst these digital natives in later life as computing becomes ever more pervasive, as is the case with other more established technology in the home and at work. Unless users of the internet develop an interest in social computing and the effects technology can and does have on our everyday lives, they may never realise how their trail of interaction could lead to problems in their future. Indeed, as mentioned in the introduction to chapter 3, it may not necessarily be the user themselves entering the data; often, through such things as social networking sites, comments are made about us without our knowledge. As will be discussed later in this chapter, it is therefore imperative that those interested in gaining a more detailed insight into our online reputation also learn to distinguish the truth from the gossip and rumour, but how this can truly be determined is difficult to know.

As examined in section 2.4, if the early vision of a semantic web by Tim Berners-Lee, the creator of the internet, comes to fruition and the internet becomes more pervasive in our daily lives, the minutiae of our choices could have unforeseen future ramifications. These will be discussed further in the following sections of this chapter, but an example might be that the choice of an unhealthy food item automatically regularly ordered by our networked refrigerator, could lead an automated vetting system utilised by our health insurance provider to raise our premiums.

6.1 Corporate Use Of Personal Internet Data

There is growing evidence (see section 3.3) that employers are utilising the internet to gain a better understanding of those applying for a particular post, and to monitor current employees for any potential misdemeanours such as discussing company business in the public domain. It is difficult to know the actual number of employers performing these searches on potential and current employees; a research study performed by the UK based recruitment agency Poolia in 2007 stated their findings at approximately 66% of those polled, whereas only 7.5% of the clients polled by another recruitment agency, Crone Corkill, admitted to regularly using the internet for 'value-added' information (see section 3.3). Whilst this does not give a clear view of the number of those organisations accessing our personal information, it at least goes some way to providing us with proof that the process exists. What could be assumed from the results of these two research studies is some detail on the types of employer who may or may not be interested in a person's internet reputation. Poolia's main clients are those working in the financial services sector (Poolia, n.d.) and therefore employees would normally be required to have a certain amount of trustworthiness and educational standards. In comparison Crone Corkill deal mainly with the recruitment of office support staff (Crone Corkill, n.d.) and historically, anecdotal evidence shows that there are those that assume these roles are of less importance generally in the workplace. What can be seen from these results is that the varied industry sectors possibly treat the use of cyber-vetting, if used at all, in differing ways, and therefore job seekers should take this into consideration prior to their application. A private discussion between the author and an IT sector employer attending the 2009 student project conference

(company name omitted for privacy reasons), confirmed that they regularly use cyber-vetting when recruiting technical staff.

Employers and recruiters need to show some prudence when using candidate data sourced from anything other than their formal application and CV documents. If candidates feel that they have been actively discriminated against based upon the contents of their NetRep (see glossary chapter 9 for clarification) they may be able to take legal action against the company concerned. In addition to this, if any personal information is printed and stored alongside an application, the organisation could find they are in breach of the Data Protection Act (see section 4.2.1), especially if this is directly related to the candidate's gender, sexual orientation, personal beliefs or disability status (Black, n.d.). It is imperative though, that recruiters and employers also understand that not all of the information found may necessarily be written by the individual being researched. If you have a very common name there could be some confusion over whether the entry could be directly linked to you personally, or the entry could prove to be part of a spoof or malicious hoax. Examples have been found where students have created fictional social network profiles of their teachers containing "pornographic photos and offensive comments" (Solove, 2007, p38-39).

University students may be more at risk from information sourced through their personal interaction with the internet (see section 3.4), as in many cases their use of social networking and collaboration tools is almost second nature. From discussions with fellow students, many do not seem to believe that employers may search the internet specifically to gain a better understanding of the person as a whole, as part of their recruitment process, even if an informal one. Their university life may have contained a mixture of study and social activities, which at the time made the overall experience more enjoyable, but once they move into a more professional environment the public details of some activities could be taken out of context, or contradict information included in a CV or formal application.

Simply hiding from everyone and choosing not to have any form of profile could also have an adverse effect on your reputation both on and off line. It is

conceivable that employers could consider a younger person who appears not to have any form of online profile to be some form of outsider, be un-skilled in terms of technology knowledge and usage, or that they may have something to hide; the same may be said of profiles which have been completely blocked to those not on your friend list. Having separate professional and personal profiles can be a good idea if they complement each other; if they do not, it could be seen as a sign of a split personality by both employers and friends (“Can Social Networking be good...”, 2008). In the authors view, an effective method of managing your ‘NetRep’ may be to look at your online presence from the point of view of both a current or prospective employer, and of your friends. Are you ensuring that you paint a favourable picture of yourself from a professional perspective when searching for employment, whilst still maintaining your public personality? A continuation of the employer discussion at the recent project conference confirmed that it can be seen as unusual for IT and computing students not to have some form of viewable profile, especially when it comes to their professional lives. If for instance someone were to apply for a position as a graduate web developer, there would be a strong expectation by the prospective employer for the candidate to have a portfolio of their work, available electronically at least but more likely online, as evidence of prior knowledge. This assumption could also be transferred to other IT roles in that applicants may need to evidence their working knowledge of the internet and its associated applications through example.

Once in employment, a person should still consider how their actions may have a detrimental effect on their future career. Corporate surveillance of employees is managed in many organisations by the implementation of acceptable use policies (AUP’s) as part of the agreed contract of employment. As noted in section 3.5, it is not necessarily the efficiency of staff and their effective use of working time that concerns employers, but the possible loss of confidential data, and the potential for some employees to take the opportunity of free internet access to download illegal or inappropriate content or submit comment, slighting their employers, onto social networking or blog sites. Thought should be given to these possibilities, and others, when an organisation is creating an AUP for the first time. As a way of mitigating risk, employee access to particular websites, or groups of websites, could be provided either during restricted times, or from ‘dumb’ terminals where

there was no possibility of any malicious access to the corporate network. The AUP would then qualify to staff that this access had been provided to show trust, but that it would be monitored as per the corporate guidelines (Naylor, 2008, p4-5). Hampshire County Council has recently been discussed in the national news for threatening their staff with an overarching ban on the use of the social networking website Facebook. “Bosses said they noticed an increase in use and during monitoring 46 employees were found to have regularly spend more than an hour on the site each day” (“Council staff face Facebook ban”, 2009). This article shows how employee monitoring can locate the worst offenders in any organisation. There is no information on whether this monitoring was undertaken as part of an AUP; however the council may wish to ensure that these findings have no detrimental effect on their public image, and on staff wellbeing and morale. The situation could perhaps be better managed by offering staff time-limited access to certain websites ensuring they were only used during scheduled breaks. In addition to managing personal use of the internet during working hours, managers at Hampshire County Council perhaps need to consider their opinion of collaborative working. If employees are using these social networking tools to contact fellow employees, then perhaps the Council needs to consider implementing specific technology to assist with team working.

As has been noted in section 3.6, a growing number of organisations are now looking towards providing approved social networking tools as part of their move towards a collaborative working environment. There must of course be a proven business need for these tools, and staff may need some encouragement to use them; however, properly used networking tools integrated with current systems and processes could enhance working lives, and provide efficiency gains. For some employees, a tool such as instant messaging could make their working lives easier. There are times when a simple, short answer is required from a colleague, and to find and speak to someone in person could take valuable time away from working. In larger companies, providing staff with a system where they can not only contact each other online, but also see a photo of a colleague prior to an important meeting, may help ease the working process and any initial nervousness experienced by newer employees (“Bosses ‘should embrace Facebook’”, 2008). There are many possible uses for networking tools within business, and they could be regarded as the natural next step to corporate

growth, but as with the use of social networking tools within a working environment, employees need to be trained in correct etiquette. Open, and quite different, profiles on both business and social networks may allow some to easily find the links between them, and other people may suffer through association.

6.2 The Law, The Government And Corporate Access To State Data

Chapter 4 of this project provided information on how personal information stored by the government, on a variety of databases could add to our overall virtual shadow. When considering the effect this data could have on employability the author felt it important to first provide some evidence on how private information can be found in a public domain. Whilst it may not be surprising that data is occasionally lost (see section 4.1), the ongoing process to merge previously separate databases may mean that these data losses could become more important on a personal level. Disreputable members of society may be using this lost data to commit identity fraud in a myriad of ways, which in turn could lead to errors being made within other online records. If found by an employer and not properly investigated to ensure its relation to a particular applicant, this case of mistaken identity may lead to loss of access to certain roles especially those requiring security clearance. This is however a dystopian 'worst-case' viewpoint, but is still something we should all be aware of.

One of the more controversial databases currently used by the government holds DNA information on approximately 4.5 million citizens ("Baby's DNA...", 2009). Many of these records relate to those who have not been convicted of a crime and, as recently reported on the BBC News website, one entry relates to an infant of less than 1 year old (Ibid). Section 4.1.2 provided other examples of the type of person who may find their DNA being held for longer than initially anticipated. Whilst this may not appear to have any direct link to employability, it is still part of our overall virtual shadow. As more employers insist on medical testing prior to commencement of employment, how long will it be before applicants are actively discriminated against for something found within their DNA profile, and over which they have no control. Databases containing genetic profile information on individuals could be used by employers to victimize those found to have a susceptibility to mental and physical complaints. "In February 2002 Norwich Union Life, one of Britain's largest insurers, admitted using genetic

tests for breast and ovarian cancer and Alzheimer's disease to evaluate applicants" (Öqvist, 2009, p143). If these tests were to be undertaken during the employee medical clearance process, the organisation could find themselves subject to higher insurance premiums making the applicant a poor risk. With these profiles mainly used during criminal cases, is it also possible that the innocent could be discriminated against simply because their DNA is held by the government and they are therefore assumed to have had a criminal conviction; only those with direct access may know if the records contain information on whether the record was originally stored for prosecution purposes, or to remove an innocent from investigation.

The UK Data Protection Act (DPA) is there to protect the populous from unauthorised and unscrupulous use of their personal information; however it does not appear to cover data transferred abroad as part of a globalised corporation. As many of us may have experienced when calling our bank or insurer, the call centres are quite often located in foreign locations such as India. Only by reading the small print in the associated terms and conditions may we find reference to our data protection rights. Individuals have to place their trust not only in the corporation that we openly give our details to, but also in the networks that transfer this information. As noted at the end of section 4.2.1 however, the government are already discussing ways of making the sharing of personal digital information easier to manage.

Clause 152 of the Criminal and Justice bill, although temporarily suspended, would allow for the sharing of data between government agencies and private corporations so long as there was a specific legal requirement. Referring back to the possible future use of the DNA database in employee medical testing, this clause would allow for the automatic transfer of a patients medical records from the NHS to a private insurance company without prior consent. Whilst assisting with false insurance claims, it could also provide employers with further reasons to not continue with a particular application for employment. "In effect, these amendments would permit a Minister to allow any person (including a company or another government department) to share information about any person (including company information) as well as personal information that they hold on any person (e.g. name, address, date of birth, ethnicity, credit history, medical

records, DNA and genetic information, tenancy records, social work records etc), if to do so serves the government's policy objectives" (Privacy International, 2009, p12). This would potentially add an immense amount of information to our already overcrowded virtual shadow, and could lead to many ways of denying access to certain employment such as that requiring security clearance. Elements of clause 152 also provide some back-up to the Regulation of Investigatory Powers Act (RIPA) in that it would allow for the "[r]outine sharing of information from government departments to the intelligence and security services without parliamentary approval" as well as "[f]ull disclosure of telecommunications data from service providers to government" (Privacy International, 2009, p5). As found in the Joseph Rowntree report into the 'database state, up to a quarter of the forty-six government databases investigated appeared to be in breach of both the DPA and personal human rights, and the ratification of clause 152 would have made these legal in the eyes of the UK law (Evans, 2009).

7 Conclusion

7.1 Research Questions

The original research questions associated with this project, as noted in the introduction, have been extensively discussed within the preceding chapter. By way of conclusion a precise summary of the answers to these questions, based on the evidence provided, is shown below.

7.1.1 What Is Web 2.0 And Why Is It So Important?

The importance of Web 2.0 to this project was detailed in chapter 2 and covers the use of social networking, wiki's and blogging tools. It is imperative that internet users understand the workings of these before they can truly comprehend the possible implications on their future employment prospects.

7.1.2 What Is A Digital Footprint?

A digital footprint, as outlined in section 2.2, is a name given to the records made of our dealings with the internet. These are directly related to personally identifiable information personally left during regular internet usage and/or interaction with Web 2.0 applications.

7.1.3 What Is A Virtual Shadow And How Is This Relevant To Workplace Surveillance?

Again as outlined in section 2.2, a virtual shadow is an extension to the personally made digital footprint. This would include comment left by others on our behalf either as part of their own digital footprint, or as part of a fictional or spoof profile deliberately created to cause harm. It can also relate to personal data stored, and in some cases shared, by both the government and private corporations. Employers are increasingly utilising the internet for value-added information on applicants, and also to ensure that current employees are not leaving defamatory comment on a public domain.

7.1.4 Is There Evidence That Prospective Employers And Recruitment Agencies Utilise The Internet For Background Checks On Applicants During Any Recruitment Process?

As this report describes, there is anecdotal and other evidence, found during secondary research, of employers using the internet during the recruitment process, however none of those approached formally were willing to directly participate in the primary research associated with this project. The only direct and related comment from an employer was made verbally during the student project conference in March 2009, and informally confirmed that the practice takes place, but that its use is the personal choice of individual employers, rather than something which may be included in corporate recruitment or HR policy. It is therefore unregulated and informal. Chapter 3 along with its associated discussion in section 6.1 provide some of this evidence and its relevance to employability.

This form of privacy invasion by prospective employers is further reflected upon in section 7.2; however it should be noted that any formal corporate, or legal guidelines on this practice would prove hard to enforce, due to the personal information being held in the public domain. Perhaps this should therefore be considered a moral issue as prior to the creation of the internet employers did not necessarily seek out details of the personal lives of employees, either potential or actual. A further question that could be asked is whether individuals have the right to both a digital work footprint and a digital life footprint, with each having no influence over the other. Many of us may conceivably have done something which may be perceived as wrong in someone else's eyes, and details of these actions, for some individuals, have been found on the internet by an employer or potential employer. Should this information therefore be used to give an appraisal of your personality, or does it say more about the personality of the person drawing conclusions and perhaps making an accusation based on this information.

7.1.5 Can Some Employee Interaction With Web 2.0 Applications Be Beneficial To Business?

As discussed in section 3.6, in a collaborative working environment Web.2.0 style applications can be of major benefit to business in a myriad of ways. Some employers have created their own versions of social networking tools allowing employees to enhance their knowledge of a colleague prior to an important meeting, and others are using public tools such as Facebook to augment their recruitment process. Sales and marketing staff are also using tools such as LinkedIn to replace their 'black books' of client data and to expand their network of contacts.

7.1.6 What Personal Data Is Stored And Potentially Used By The State Within The UK And Globally With Regard To The Workplace?

Chapter 4 examined the use of personal data by the government along with the various laws enacted to protect its citizens. The security services are currently allowed, by law as part of the RIP Act (2000), to access the internet usage profiles of targeted individuals upon request. These targeted individuals could be any member of society who has come to the attention of the security services for whatever reason, and these usage profiles are therefore required for investigative purposes. What is important to note, is that incorrect data held by government agencies could lead to refusal of security clearance and therefore certain types of employment. If clause 152 of the Coroners & Justice Bill is approved the government and private organisations will have further access to personal information from shared databases, some of which is in direct conflict with the current Data Protection Act (DPA).

7.2 Project Reflections and Future Issues

Whilst this report may seem to paint a particularly dystopian view of data security, one important point to come from this research project is that we as individuals need to understand how our personal information can be both collected and used by others for different purposes. Since the inception of the internet and the interconnected world that we live in, we have been leaving small footprints behind us as we wander through cyberspace; small records of our interaction with others online. The growth in the capacity of data storage and the ever lowering costs

involved, is leading to more information being stored for longer. There is no such thing as 'delete deleted' on the internet; you may have removed your profile from a social network, but your original online friends will still have data relating to your interactions with them, they may still have copies of those embarrassing photos you never want anyone to see. What we all have to know is how to manage our online reputation both from the past and in the future. As the internet becomes ever more integrated into our lives, it could prove easy to become apathetic about our online reputation, but if you are looking for employment, especially with a technology company, you should become more aware of what should and shouldn't be easily found online about you. As an example, anyone looking for a role as a web developer needs to have an online portfolio as a basic addition to their curriculum vitae, to illustrate their skills and competencies. Others might consider keeping a more detailed resume online on a personal webpage which could expand on past experience, offer links to previous employers and be referenced on any application. Again consider how much detail to include in your online resume; whilst it is important to ensure an employer can gain a deeper understanding of your education and experience, consideration should still be given to what personal contact details are used, to prevent this information being used by an unscrupulous party, for example as part of an identity theft attempt.

Employers and recruitment agencies need to show prudence when searching online sources for enhanced personal data on applicants, and should ensure that the information they may be reviewing is not part of a malicious attack on an individual, or a fictional profile. If an applicant decides to investigate further the reasons behind the refusal of an interview, they have particular rights under the Data Protection Act 1998 to any information held on them by an organisation. If the refusal is shown to be based upon any racial, sexual or other discrimination they have the right to commence legal action against the company involved. It is possibly for this reason that organisations are nervous about confirming the use of internet profiling during recruitment, but they still have to show a definitive reason why an applicant was refused, especially if they have the exact experience and knowledge required on the original advertisement.

The UK government, whilst appearing to be providing legislation to further protect our personal information online, are themselves exempt from these laws. The

merging of databases containing personal information is allowing for the future possible profiling of citizens, and could lead to such things as a refusal for credit because of something stored within the very building blocks of our lives, our DNA. If clause 152 of the Criminal and Justice Bill is accepted into law we will all be expected to provide DNA and other biometric information which will be used to track our movements. A simple error in one of these records could lead to the refusal of security clearance for employment as varied as the police, teaching or working in healthcare. These are elements of our virtual shadow which we have almost no control over, but having the ability to recognise when something is wrong at an early stage will ensure the future safety of our data. There is much confusion surrounding digital identity, and this therefore can make it difficult for any individual to properly understand how much personal data may be stored within government databases. What is of concern, and should be understood by all UK citizens, is that many of the government databases not only contravene data protection laws, but also have the potential to breach our human rights.

Finally it is worth noting that many of us may be guilty of giving away some personal details without considering the implications, where there is the possibility of some form of prize. Marketers have long known this and many brands use giveaways to tempt us into giving details such as our mobile phone number, name and address. Current examples include the KitKat Perfect Break (Nestle, 2009), and the Coca-Cola Zone Big Match Giveaway (Coca-Cola, 2009). We can all be blind to the multitude of uses our personal information could have to others, but as long as we have some knowledge and appreciation of this we can start to ensure our own safety. On a more positive side, the sharing of simple information with others could lead to a free holiday or the growth of our network of friends. No single person or group has overall responsibility for ensuring that citizens have the knowledge required to manage their online profiles, although the government have published various guidelines. Taking this into account, we should all therefore be responsible for our own actions online, and be prepared to manage any problems that may arise whether directly related to personal employability, or any other area of our lives.

Future research into the subject of this project could include an investigation of the use of social networking and Web 2.0 style tools in a working environment.

Some organisations have already embraced the use of these tools in varying ways; however it may be interesting to confirm how much these are used by staff and what the perception is of them generally, along with the identification of any real or tangible business benefits that the use of these tools may offer. A more technical version of this project could include the creation of a 'sniffer' programme to perform internet searches for named individuals automatically, providing a single, simple list of findings from an examination of many different websites. An employer at this year's student project conference confirmed during our discussion that this would be a useful time saving tool, thus providing some proof that there may be a demand for this form of application. This tool however may be considered as a future destroyer of reputations, rather than simply as an efficient way of searching for digital footprints and an individual's general online presence. Would this tool therefore be socially desirable? As mentioned in section 7.1.4, this could be construed as an invasion of our personal privacy, and makes the assumption that work is a major part of many people's lives. But, should career progression be determined by our personal life? Historically employers had little or no information about an employee's personal situation, other than that explicitly requested, and simple things like marital status were of no importance. However these details can now be easily found and disseminated via the internet. Although the active discrimination of employees and potential employees on the grounds of their personal choice or any medical issues is illegal in the eyes of the law, information not directly provided can easily be found through this digital backdoor. The ever increasing use of this dubious link between our personal and work lives should therefore be managed through the use of formal guidelines, or within a law such as the DPA to govern what employers are allowed to access and for what use.

8 Bibliography

- A brief history of Web 2.0 (n.d.). *Information Week*. Retrieved November 11, 2008 from http://www.informationweek.com/1113/IDweb20_timeline.jhtml
- Agarwal, N & Liu, H. (2008, June). Blogosphere: research issues, tools, and applications [Electronic Version]. *ACM SIGKDD Explorations Newsletter*, 10(1), 18-31.
- Anderson, N. (2006, September). Tim Berners-Lee on Web 2.0: "Nobody even knows what it means". *Ars Technica*. Retrieved December 2, 2008 from <http://arstechnica.com/news.ars/post/20060901-7650.html>
- Angermeier, M. (2005, November). *Web 2.0, Library 2.0 and the Future for Library Systems – Slide 18*. Retrieved November 3, 2008 from <http://digital.library.adelaide.edu.au/dspace/bitstream/2440/14789/1/Web2.0.pdf>
- Baby's DNA was held on database. (2009, March). *BBC News*. Retrieved March 13, 2009 from http://news.bbc.co.uk/1/hi/uk_politics/7933753.stm
- Berners-Lee, T. (1996). *The World Wide Web: Past, Present and Future*. Retrieved December 2, 2008 from the World Wide Web Consortium site at <http://www.w3.org/People/Berners-Lee/1996/ppf.html>
- Black, N. (n.d.). *The Employer's Guide to Blogging Pitfalls*. Retrieved August 30, 2008 from the Careers in Recruitment website at <http://www.careersinrecruitment.com/recruiters/blogging.php>
- Boggan, S. (2007, February). *No more secrets*. Retrieved November 3, 2008 from the Guardian website at <http://www.guardian.co.uk/politics/2007/feb/27/idcards.immigrationpolicy>
- Bosses 'should embrace Facebook'. (2008, October). *BBC News*. Retrieved December 2, 2008 from <http://news.bbc.co.uk/1/hi/business/7695716.stm>
- Calleja, R. (2000). RIP Act 2000 – UK [Electronic version]. *Computer Law & Security Report*, 16 (6), 400-401
- Can Social Networking be good for your Career? (2008, August). *Vista News*. Retrieved November 12, 2008 from <http://rockyourcareer.wordpress.com/2008/08/22/can-social-networking-be-good-for-your-career/>
- Can social networking expand your candidate pool? (2008). *Jobsite* [Electronic Version]. Retrieved November 2, 2008 from http://www.jobsite.co.uk/whitepaper/socnet_web.html
- CareerBuilder.co.uk (2008). *Top Trends of 2008*. Retrieved November 13, 2008 from http://www.careerbuilder.co.uk/Article/CB-106-Job-Search-Top-Job-Trends-for-2008/?sc_cmp1=JS_UK_CA_A106

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

Ceridan. (2007). *Social networking and recruitment*. Retrieved August 30, 2008 from the Ceridan Corporation website at <http://www.ceridian.co.uk/hr/newsletter/nav/1,4813,593,00.html>

Clarke, R. (1988, May). Information Technology and Dataveillance [Electronic version]. *Communications of the ACM*, 31(5), 498-512.

Clarke, R. (2009). Roger Clarke's Dataveillance and Information Privacy Home-Page. Retrieved November 10, 2008 from <http://www.rogerclarke.com/DV/>

Coca-Cola. (2009). *The Big Match Giveaway*. Retrieved March 19, 2009 from <http://www.cokezone.co.uk/home/catalogue/reward/prod870001/Sport/Big+Match+Giveaway>

Cole, M. (2009). Using Wiki technology to support student engagement: Lessons from the trenches [Electronic Version]. *Computers & Education* 52(2009), 141-145.

Conway, L. (2008). *Virgin Atlantic sacks 13 staff for calling its flyers 'chavs'*. Retrieved November 10, 2008 from the Independent newspaper website at <http://www.independent.co.uk/news/uk/home-news/virgin-atlantic-sacks-13-staff-for-calling-its-flyers-chavs-982192.html>

Cope, N. (2000). *Forget the shopping list, let the fridge order the milk*. Retrieved December 5, 2008 from <http://www.independent.co.uk/news/business/analysis-and-features/forget-the-shopping-list-let-the-fridge-order-the-milk-637847.html>

Crone Corkill. (n.d.). *History*. Retrieved March 10, 2009 from <http://www.cronecorkill.co.uk/dpages/6/history.php>

Database State. (2009, March). *Joseph Rowntree Reform Trust Ltd*. Retrieved March 25, 2009 from <http://www.jrrt.org.uk/uploads/Database%20State.pdf>

Data Protection Act. (n.d.). *Information Commissioners Office*. Retrieved February 18, 2009 from http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Data protection and identity theft. (n.d.). *DirectGov*. Retrieved February 10, 2009 from the DirectGov website at http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG_10031451

Dessimoz, D., Richiardi, J., Champod, C. & Drygajlo, A. (2006). Multimodal biometrics for identity documents [Electronic version]. *Forensic Science International* 167(2-3), pp154-159

Directgov demonstrates financial and other benefits to local authorities. (2005). *Directgov*. Retrieved February 10, 2009 from the eGov Monitor website at <http://www.egovmonitor.com/node/276>

Employers turn to Facebook. (2007, October). *Financial Search & Selection*. Retrieved August 30, 2008 from the FSS website at <http://www.fss.co.uk/prs/press-centre-details59.php>

Ernst & Young Careers. (n.d.). *Facebook*. Retrieved January 26, 2009 from <http://www.facebook.com/home.php?ref=home#/ernstandyoungcareers?sid=8569b97b9666d0399ef32312d0698524&ref=s>

Evans, D. (2008, November). *Government data losses; all part of life's rich tapestry*. Retrieved November 10, 2008 from <http://www.bcs.org/server.php?show=ConBlogEntry.735>

Evans, D. (2009, March). *Legalising the Database State*. Retrieved March 25, 2009 from <http://www.bcs.org/server.php?show=ConBlogEntry.1025>

Facebook. (2008). *Press Room*. Retrieved December 5, 2008 from <http://www.facebook.com/press/product.php#/press.php>

Gantz, J.F., Chute, C., Manfrediz, A., Minton, S., Reinsel, D., Schlichting, W. & Toncheve, A. (2008, March). *The Diverse and Exploding Digital Universe*. An IDC White Paper [Electronic Version] retrieved February 12, 2009 from <http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>

Gibson, W. (1984). *Neuromancer*. London: Grafton

Global Top Sites. (2009). *Alexa.com*. Retrieved December 5, 2008 from http://www.alex.com/site/ds/top_sites

Glossary of Technologies and e-Learning Terms. (n.d.). Retrieved December 12, 2008 from the Plymouth University website at www2.plymouth.ac.uk/distancelarning/course/glossary.doc

Government sites infected with virus. (2008). *British Computer Society*. Retrieved November 10, 2008 from <http://www.bcs.org/server.php?show=ConWebDoc.20315>

Halpern, D., Reville, P.J. & Grunewald, D. (2007). Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace. *Journal of Business Ethics* (2008) 80:175-180.

Hasan, I. (2007, May). Watching the detectives [Electronic Version]. *Solicitors Journal*, 151(20).

Hinchcliffe, D. (2006, September). *All we got was Web 1.0 when Tim Berners-Lee actually gave us Web 2.0*. Retrieved December 3, 2008 from http://web2.socialcomputingmagazine.com/all_we_got_was_web_10_when_tim_bernerslee_actually_gave_us_w.htm

Hinsliff, G. (2008, March). *MI5 seeks power to trawl records in new terror hunt*. Retrieved November 3, 2008 from the Guardian website at <http://www.guardian.co.uk/uk/2008/mar/16/uksecurity.terrorism>

History of wikis. (2008, November). *Wikipedia*. Retrieved December 5, 2008, from http://en.wikipedia.org/w/index.php?title=History_of_wikis&oldid=251042016

Home Office. (n.d.). *About RIPA*. Retrieved February 19, 2009 from the Home Office website at <http://security.homeoffice.gov.uk/ripa/about-ripa/>

How social networking sites can derail your job search. (2007, February). *Resume Solutions*. Retrieved November 3, 2008 from <http://resumesolutions.wordpress.com/2007/02/08/how-social-networking-sites-can-derail-your-job-search/>

Identity Cards Act (2006). Retrieved March 5, 2009 from the Office of Public Sector Information at http://www.opsi.gov.uk/acts/acts2006/ukpga_20060015_en_1

Jardin, X. (2009). *Online social networks go to work*. Retrieved January 26, 2009 from <http://www.msnbc.msn.com/id/5488683/>

Joinson, A. & Whitty, M. (2008, Jan). Watched in the workplace [Electronic Version]. *Info Security* 5(1), 38-40

Jones, L. (2008). *The Dark Side of the Internet*. Unpublished internal document, University of Portsmouth.

Kelly, S. (2008). *The spread of our 'digital footprint'*. Retrieved December 12, 2008 from the BBC Click website at http://news.bbc.co.uk/1/hi/programmes/click_online/7380645.stm

Kennedy, J. (2008). *When social networking goes bad*. Retrieved November 4, 2008 from the Silicon Republic website at <http://www.siliconrepublic.com/news/news.nv?storyid=single10608>

Leighton, P. & Proctor, G. (2006). *Effective Recruitment: A practical guide to staying within the law*. London: Thorogood Publishing Ltd.

Lewis, D. (2006). What is Web 2.0? [Electronic version]. *ACM Crossroads*, 13(1), 3-13

LinkedIn. (2008). *About Us*. Retrieved January 26, 2008 from <http://press.linkedin.com/about>

List of social networking websites. (2008, December). *Wikipedia*. Retrieved December 5, 2008, from http://en.wikipedia.org/w/index.php?title=List_of_social_networking_websites&oldid=255828522

Lyon, D. (2003). *Surveillance as social sorting: privacy, risk and automated discrimination*. London: Routledge

McCarthy, K. (2000). *TUC gets arsey about RIPA email laws*. Retrieved November 3, 2008 from The Register website http://www.theregister.co.uk/2000/11/17/tuc_gets_arsey_about_rip/

McFedries, P. (2007). *Googleability*. Retrieved January 15, 2009 from the Word Spy website at <http://www.wordspy.com/words/googleability.asp>

Metz, C. (2007, April). Web 3.0: The internet is changing again. *PC Magazine* 4/10/2007 26(7/8), 74-79

Mostrous, A. & Brown, D. (2008). *Microsoft seeks patent for office 'spy' software*. Retrieved December 1, 2008 from the Times Newspaper at http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece

Myron, M. (2008). *What is Privacy?* Unpublished undergraduate dissertation, University of Portsmouth, Portsmouth.

Nash, E. & Arnott, S. (2004, July). *New passport database will tie in with ID cards*. Retrieved November 3, 2008 from <http://www.vnunet.com/computing/news/2070787/passport-database-tie-id-cards>

Naylor, J. (2007). *Online social networking: The employer's dilemma - MessageLabs whitepaper [Electronic Version]*. Retrieved December 2, 2008 from the MessageLabs website at http://www.messagelabs.co.uk/whitepaper/socialnetworking_legal_A4_UK.PDF

Naylor, J. (2008). *Email compliance: Email use and misuse within the workplace - MessageLabs whitepaper [Electronic Version]*. Retrieved December 2, 2008 from the MessageLabs website at http://www.messagelabs.co.uk/whitepaper/EmailCompliance_Final_A4.pdf

Nazir, A., Raza, S. & Chuah, C. (2008). Unveiling Facebook: a measurement study of social network based applications [Electronic Version]. *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, 43.56

Nestle. (2009). *KitKat Perfect Break*. Retrieved March 19, 2009 from <http://www.kitkat-perfectbreak.co.uk/Front/>

Norton-Taylor, R. (2008, October). *New powers for state snoopers on the net*. Retrieved November 3, 2008 from the Guardian website at <http://www.guardian.co.uk/technology/2008/oct/16/internet-uksecurity>

Online Social Networking: What it really means to Employee Recruitment. (2008, February). *Online Recruitment*. Retrieved August 30, 2008 from the onrec.com website at <http://www.onrec.com/newsstories/20445.asp>

O'Reilly, T. (2005). *What is Web 2.0? Design patterns and business models for the next generation of software*. Retrieved November 26, 2008 from the O'Reilly Media Inc. website at <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1>

Öqvist, K.L. (2009). *Virtual Shadows: Your privacy in the Information Society*. UK: British Computer Society

Paton, N. (2007). *Ever been cyber-vetted?* Retrieved November 3, 2008 from the Times Online website at http://business.timesonline.co.uk/tol/business/career_and_jobs/article1758122.ece

Personal information toolkit. (2007, January). *Information Commissioners Office* [Electronic version]. Retrieved February 19, 2009 from http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/toolkit.pdf

Pilgrim, C.J. (2008). Improving the usability of web 2.0 applications [Electronic Version]. *Conference on Hypertext and Hypermedia, Proceedings of the nineteenth ACM conference on hypertext and hypermedia*, 239-240

Poolia. (n.d.). *Our service areas*. Retrieved March 10, 2009 from <http://www.poolia.co.uk/clients/our-service-areas.html>

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. [Electronic Version]. *On the Horizon* (9)5, 1-6.

Privacy International. (n.d.) *Communications surveillance*. Retrieved December 15, 2008 from [http://www.privacyinternational.org/index.shtml?cmd\[342\]\[\]=c-1-Comms+Surveillance+Home+Page&als\[theme\]=Comms%20Surveillance%20Home%20Page&conds\[1\]\[category.....\]=Comms%20Surveillance%20Home%20Page&als\[_parent\]=Communications%20surveillance](http://www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Comms+Surveillance+Home+Page&als[theme]=Comms%20Surveillance%20Home%20Page&conds[1][category.....]=Comms%20Surveillance%20Home%20Page&als[_parent]=Communications%20surveillance)

Privacy International. (2009). *UK Data Sharing Report*. Retrieved March 13, 2009 from http://www.privacyinternational.org/countries/uk/uk_data_sharing_report.pdf

Public Bill Committee. (2009, March). *Coroners & Justice Bill*. Retrieved March 13, 2009 from <http://www.publications.parliament.uk/pa/cm200809/cmpublic/coroners/090310/am/90310s01.htm>

Regulation of Investigatory Powers Act 2000. (2006). *Warwick University*. Retrieved January 13, 2009 from the Warwick University IT Services website <http://www2.warwick.ac.uk/services/its/policies/ripa/>

Slack, J. (2007, March). *Don't like ID cards? Hand over your passport*. Retrieved March 5, 2009 from <http://www.dailymail.co.uk/news/article-441329/Dont-like-ID-cards-Hand-passport.html>

Solove, D.J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven and London: Yale University Press

Sophos (2007, August). *Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves*. Retrieved December 5, 2008 from the Sophos website at <http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html>

- The 24-hour employee? (1999, Feb). *Evolving Enterprise*, 2(1). Retrieved January 13, 2009 from <http://www.lionhrtpub.com/ee/ee-2-99/outlook.html>
- The British Computer Society. (n.d.). *Facebook*. Retrieved November 10, 2008 from <http://en-gb.facebook.com/pages/The-British-Computer-Society-BCS/26238475399>
- The National Curriculum for 5 to 11 year olds. (n.d.). *DirectGov*. Retrieved March 5, 2009 from the DirectGov website at http://www.direct.gov.uk/en/Parents/Schoolslearninganddevelopment/ExamsTestsAndTheCurriculum/DG_4015959
- The RIP Act. (2000, October). *Guardian.co.uk* Retrieved November 3, 2008 from <http://www.guardian.co.uk/world/2000/oct/24/qanda>
- Toffler, A. (1981). *The Third Wave*. London: William Collins Sons & Co. Ltd.
- Turkle, S. (1995). *Life on the Screen*. New York: Simon & Schuster Paperbacks
- Tynan, D. (2008). *Five ways to defend your online reputation*. Retrieved November 18, 2008 from the PC World website at http://www.pcworld.com/article/142721/five_ways_to_defend_your_online_reputation.html
- Vincent, M. (2007, May). *The World of Work, How cyber-vetting catches job liars*. Retrieved February 23, 2009 from http://www.spectator.co.uk/the-magazine/business/30674/part_2/how-cybervetting-catches-job-liars.thtml
- Web 2.0. (2008, December). *Wikipedia*. Retrieved December 2, 2008, from http://en.wikipedia.org/w/index.php?title=Web_2.0&oldid=255422943
- What is security clearance? (n.d.). Retrieved February 10, 2009 from http://www.securityclearedjobs.com/how_to_become_security_cleared.asp
- Wikipedia. (2008, December). *Wikipedia*. Retrieved December 5, 2008, from <http://en.wikipedia.org/w/index.php?title=Wikipedia&oldid=256017015>
- Woods, J. (2008, December). *The Apprentice Winner Lee McQueen: 'I would never condone lying on a CV'*. Retrieved February 17, 2009 from the Telegraph website at <http://www.telegraph.co.uk/culture/tvandradio/3554180/The-Apprentice-winner-Lee-McQueen-'I-would-never-condone-lying-on-a-CV'.html>
- Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M. & Mosciroda, A. (2009). Privacy, trust and policy-making: Challenges and responses [Electronic version]. *Computer Law & Security Review*, 25 (2009), 69-83
- Verkaik, R. (2007, November). *They've got your number: State's hunger for personal data raises security fears*. Retrieved November 3, 2008 from the Independent website at <http://www.independent.co.uk/news/uk/politics/theyve-got-your-number-states-hunger-for-personal-data-raises-security-fears-758997.html>

9 Glossary of Terms

Blogosphere	A collective term for individual blogs; the world of blogs.
Clickstream	The path a user takes when navigating through the internet. This path can be used to build a profile of a web user's habits showing their current interests. The collected data can then be used for targeted advertising, or to provide security services with evidence during an investigation of terrorism for example ("The RIP Act", 2000).
Cyberspace	Term used by the author William Gibson in his novel Neuromancer and refers to the range of information available through computer networks.
Cyber-Vetting	The process of utilising the internet and online searching to determine the suitability of an applicant for a particular post (Vincent, 2007).
Dataveillance	"The systematic monitoring of people's actions or communications through the application of information technology" (Clarke, 1987).
Digital Footprint(s)	The trail of information personally left during regular internet usage and/or interaction with Web 2.0 applications (Gantz et al, 2008).
Digital Immigrant	Those not born into the digital age but interested in new technology and its adoption (Prensky, 2001).
Digital Native	Those born into the digital age and introduced to technology from an early age (Prensky, 2001).
Digital Shadow	See Virtual Shadow
DPA	Data Protection Act 1998 (updated from 1984 Act)
Googleability	A colloquial term becoming more frequently used meaning "the ease with which information about a person can be found on an internet search engine, particularly Google" (McFedries, 2007)
LSC	Learning & Skills Council of the UK (http://www.lsc.gov.uk)
Meatspace	A term used by William Gibson in his 1984 novel Neuromancer when describing real life. This was intended to be the opposite of Cyberspace.
NetRep	The outcome of cyber-vetting, or a person's internet reputation (Paton, 2007).
RIPA	Regulation of Investigatory Powers Act 2000

Viral Marketing	A marketing technique that relies on personal social networks for the transfer of brand awareness information. Examples include simple games, video or animations.
Virtual Shadow	An accumulation of digital footprints left behind during internet use, along with other digitally stored information such as CCTV images and state and criminal records (Öqvist, 2009).

10 Appendices

10.1 Research Assistance Request Letter

10.1.1 Employers

HR Recruitment Manager

10 November 2008

Dear Sir/Madam,

I am a mature student at Portsmouth University studying for a BSc (Hons) Computing & Society. I am writing to ask for your assistance with my final year project which is researching the use of the internet, specifically Web 2.0 applications, within recruitment and staff retention. I have found anecdotal evidence from various sources, but would be interested in hearing the views of someone in your position.

All information provided will be held in the strictest confidence and no personal or corporate names will be used in the final report.

Specifically, I would be interested in your answers to the following questions:

1. Does your company allow the use of the internet during any recruitment process for further background checks on applicants, and is this corporate policy?
2. If yes, what types of information do you endeavour to source regarding the applicant and what applications or processes are used?
 - a. Do you 'Google' applicants?
 - b. Have you ever refused to pursue an application based on information found within the public domain of the internet?
3. If no, is this due to company policy or personal choice?
4. Has your company terminated an employment contract or formally warned an employee based on their internet use? What were the general circumstances surrounding this and was it based on an acceptable use policy?

I understand that you may not be able to provide specific answers to all of these questions, but any information you can provide would be of use to my research project.

I am also hoping to personally interview some of the people contacted during this initial part of the process. If you would be interested in providing this access to give further information it would be most appreciated.

A reply would be your consent for information to be used. If you would like to take part in the research process then you would be welcome to receive a copy of my final report after completion in May 2009. Any queries should be directed to my home address above or via one of my university e-mail addresses ecs50277@port.ac.uk or Diana.dupree@upsu.net.

Thank you in advance for your participation.

Yours faithfully,

D.M. Dupree (Mrs)

10.1.2 Recruiters

Senior Recruitment Consultant

10 November 2008

Dear Sir/Madam,

I am a mature student at Portsmouth University studying for a BSc (Hons) Computing & Society. I am writing to ask for your assistance with my final year project which is researching the use of the internet, specifically Web 2.0 applications, within recruitment and staff retention. I have found anecdotal evidence from various sources, but would be interested in hearing the views of someone in your position.

All information provided will be held in the strictest confidence and no personal or corporate names will be used in the final report.

Specifically, I would be interested in your answers to the following questions:

1. Does your company allow the use of the internet during any recruitment process for further background checks on applicants, and is this corporate policy?
2. If yes, what types of information do you endeavour to source regarding the applicant and what applications or processes are used?
 - a. Do you 'Google' applicants?
 - b. Have you ever refused to pursue an application based on information found within the public domain of the internet?
3. If no, is this due to company policy or personal choice?

I understand that you may not be able to provide specific answers to all of these questions, but any information you can provide would be of use to my research project.

I am also hoping to personally interview some of the people contacted during this initial part of the process. If you would be interested in providing this access to give further information it would be most appreciated.

A reply would be your consent for information to be used. If you would like to take part in the research process then you would be welcome to receive a copy of my final report after completion in May 2009. Any queries should be directed to my home address above or via one of my university e-mail addresses ecs50277@port.ac.uk or Diana.dupree@upsu.net.

Thank you in advance for your participation.

Yours faithfully,

D.M. Dupree (Mrs)

10.2 Student Research Conference

The conference was held on Wednesday 11th March 2009 in the School of Computing, Lion Gate Building.

10.2.1 **Abstract**

The below copy was taken from the official documentation available at the conference.

Diana Dupree	BSc Computing & Society
Digital Footprints and Employability: A critical examination of the implications of digital identity with reference to the growing corporate and state use of data regarding employees.	
<p>You may consider you have a right to personal privacy. However if you use the internet on a regular basis you may leave digital footprints: small records of your interaction with the internet which may be far from private, and which may collectively have an unwanted impact on your future. The growth of Web 2.0 technologies, such as social networking and blogging, has made it easier to digitally interact with our friends and family, as well as with others with similar interests. However the messages we leave behind in our own name, on behalf of, or discussing others can all be linked together to form a virtual shadow or online profile. Data collated about our personal lives from other digital sources such as CCTV, medical and criminal records, and information we provide government agencies, add to this profile at each interaction and can persist beyond our control.</p> <p>There is growing evidence (Career Builder, 2008) that employers are increasingly utilising the internet to gain ‘value added’ information on candidates, and are using this new information to eliminate applicants based on what they find. This project aims to make the reader aware of how their personal interaction with the internet can affect their future employability, and provide some guidance on how to manage their online profile. When sharing personal information online, particularly via Web 2.0 applications (for example social networking sites, wiki’s and blogs) we should do so in an informed way: With an awareness of how that information may be interpreted, potentially years into the future, by an external party, who may have an agenda far beyond the context in which we originally shared our information. For example, employers from a secure sector, such as law enforcement, government or the security services, may actively seek out your “virtual shadow” when considering you as a candidate. This may contain data you provided many years ago, and which you now no longer have control over, and which may portray you in a way you may not wish to be seen by a prospective employer.</p>	

Ever been cyber-vetted?

Research undertaken by a UK recruitment firm in 2007 found that two-thirds of the 500 employers polled “admitted regularly carrying out internet searches, including checking social networking sites” (Paton, 2007)

Defend Your Online Reputation

1. *Google yourself*

Search for name and address and see what you find.

2. *Comb the web*

Use other specific ‘people search’ engines to find more personal content such as social networking and electoral role details.

3. *Opt out early & often*

Check registration forms for marketing options – always opt-out!

4. *Do your own background check!*

For security vetted job applications, do a personal credit check to ensure no-one has stolen your identity.

5. *Defend your reputation*

If there is too much online material for you to remove on your own, pay someone else to look after your reputation. (Tynan, 2008)

Digital Footprints and Employability: A critical examination of the implications of digital identity with reference to the growing corporate and state use of data regarding employees.

Diana Dupree
BSc (Hons) Computing & Society

References:

- Paton, N. (2007). *Ever been cyber-vetted?* Retrieved November 3, 2008 from http://business.timesonline.co.uk/tol/business/career_and_jobs/article1758122.ece
- Tynan, D. (2008). *Five ways to defend your online reputation.* Retrieved November 18, 2008 from http://www.pcworld.com/article/142721/five_ways_to_defend_your_online_reputation.html

10.2.3 Handout

Shown below is an image of a handout given to those interested in my project. This was originally a double sided A5 document.

Five Ways to Defend Your Online Reputation

You may consider that you have a right to personal privacy. However if you regularly use the internet you may leave digital footprints: small records of your interaction which may be far from private, and which may collectively have an unwanted impact on your future. There are ways to manage your online reputation and it all starts with discovering the size of your digital footprint.

- Google Yourself**
If someone were to Google your name or address would they find out nasty things about you? "Google is not only just a search engine; it's a reputation engine" (Dellarocas cited in Tynan, 2008). The results could show personal entries and comments made by friends, family or colleagues. If the entry is something from your own website, remove it and ask Google to remove it from their search results. However, if the entry was made by someone else, you have little or no control over its removal (see item 5).
- Comb the Web**
Not everything will be captured in Google results. Ensure no spoofed social networking profiles have been set up in your name. Try using specific 'people search' engines such as Pipl, Spock or ZoomInfo to find details of your social networking profile. Remember, the profile may contain elements of profiles belonging to others with the same name as you.
- Opt out early and often**
Any registration form completed online or in print will offer an 'opt-out' option when it comes to marketing materials. Removing yourself from these lists will ensure that no junk mail or spam can be linked to your name, e-mail or home address. As an example, these could be used by identity thieves to apply for 'pre-approved' credit cards in your name.

- Do your own background check!**
Have you ever been arrested or accused of any crime? Have you ever been late with tax payments? Are you married or divorced? All of these can affect your credit rating as well as providing extra information to those investigating your reputation. Anyone applying for a position within the security services, or an organisation contractually linked to the government will normally need to undergo a level of security vetting. Any 'black-marks' against your name could deny you access not only to a secure status, but also employment.
- Defend your reputation**
Remember, you may have deleted your Facebook or MySpace account showing those naked or drunken photos of you from your time at University, but others may not. Something deleted from your account may still appear on the profile of an old friend or colleague. Take time to find these and request that they be removed. Just remember that it takes a long time for entries to be removed from search engines. If your online profile cannot be managed personally, there are companies available such as Reputation Defender.com who will take the "nuclear option" (Tynan, 2008) and find and remove these entries for you for a fee.

Diana Dupree
BSc (Hons) Computing & Society
University of Portsmouth, 2009

This handout was created with the assistance of:
Tynan, D. (2008, February). Five ways to Defend Your Online Reputation.
Accessed November 18, 2008 from the PCWorld.com website at
<http://www.pcworld.com/article/142721-2/five-ways-to-defend-your-online-reputation.html>