# Surveillance, Privacy and Technology: Contemporary Irish Perspectives

By

Kenny Doyle B.A. (Hons)

A thesis in fulfilment of the requirements
For the Masters of Arts Degree (Sociology) by Research

Waterford Institute of Technology

Research Supervisor:
Jonathan Culleton MA (Hons)

Submitted to Waterford Institute of Technology June 2013

## Abstract

Surveillance, Privacy and Technology: Contemporary Irish Perspectives

Kenny Doyle

Surveillance is typically envisaged as the act of a person being physically watched, their movements and behaviour monitored in a given space and time. While this type of watching undoubtedly takes place, there is also the more subtle and pervasive monitoring of people through the data they accumulate in their daily lives. Contemporary Irish society is mediated by digital technology; the daily life of the typical person creates a mass of data which can offer many telling clues as to the type of life they lead. This form of surveillance is called dataveillance (Clarke 1988). It is unclear however exactly how much citizens know about these practices and how they negotiate with and respond to surveillance systems which have become integrated into the everyday lived experience in Ireland. This study aimed -by conducting focused interviews with Irish citizens – to explore the levels of knowledge regarding surveillance and privacy and to ascertain the importance placed on these concepts.

Fifteen people participated in semi-structured interviews as part of this qualitative study. The interviews covered the participants knowledge of surveillance, privacy and technology in the three social roles of worker, citizen and consumer. Thus the three main themes of the interviews centred around work, security and consumption, with each theme opening up a series of discussions on normative expectations regarding surveillance and privacy. As well as exploring the level of knowledge regarding surveillance and privacy, a further aim to uncover any discursive repertoires used to describe how participants understand and interact with systems of surveillance.

Broadly speaking the findings were that there is a very basic understanding of surveillance, who it is conducted by, and the reasons for its occurrence. While participants mostly identified themselves as being private, their actions often left them open to surveillance in ways which they knew very little about. This was particularly

evident in questions relating to consumer based surveillance, social networking and use of the internet in general. There was very little in the way of knowledge about the information economy as was most strikingly evident in the fact that most participants had no idea how either Google or Facebook make money.

Many conceptions of surveillance see it in terms of it being a top down style exercise of power, as is evident from this study it is perhaps not quite so simple. Systems of monitoring and surveillance can be seen in some instances to work both ways and in the examples of both law enforcement and work supervision; surveillance was characterised as a means of holding power to account. This means that in some limited examples subjects of surveillance are capable of reflecting its gaze back on the people or organisations conducting it. In the case of work supervision for example, it was exhaustive systems of record keeping and oversight which made it easier for employees to hold their employers to terms of their contracts. In these terms workplace surveillance was welcomed as it allowed for greater transparency.

A further finding which related mostly to the realm of policing and security was that of a form of 'othering' of targets of surveillance. This was usually tied in with the almost ubiquitous subject position of if you have nothing to hide then you have nothing to fear. According to this logic it is those who are characterised as having something to hide who are the targets of surveillance and thus stand to lose out when it is in operation. This view creates a dualism in common consciousness between 'us' who obey the law and thus have nothing to fear, and 'them', drawn from the class of the criminal 'other'. The creation of such simplified and dichotomous identities ensures the social desirability of surveillance and serves to inoculate its proponents against meaningful discussion about the necessity or validity of any surveillance measures. This logic also forms part of the explanation as to why systems of surveillance have spread so rapidly without much in terms of organised public opposition.

Table of Contents

## Chapter 4: Surveillance



## Chapter 5: Surveillance and the Workplace



## Chapter 6: Surveillance, Security and the State

**Chapter 7: Consumerism**



**Chapter 8: Conclusion and Discussion**

## Chapter One. Introduction

'Information is the oxygen of the modern age' (Ronald Regan 1989, quoted in Lee 2013, p. 3)

We're an information economy. That's what they teach you in school. What they don't tell you is that it's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information. Fragments that can be retrieved, amplified … (William Gibson 1981, p. 30)

The last three decades have been defined by technological change, particularly that of information and communications technology. In particular the advent of personal computing and the internet has freed up information and communications capabilities between most people of the developed world: '[w]ith little exaggeration, we may call the 21st century the age of networks' (Van Dijk, 2006, p. 2). Technologically enabled global networks have profoundly altered our lives in almost all areas including work, consumption, entertainment and learning. Zimmer tells us however that 'the true relationship between a society and its technology is often not purely benevolent, but instead may require a sacrifice for society to enjoy its benefits' (2008, p. 111). The sacrifice of the information age is most commonly held to be personal privacy; Scott McNealy, chairman of Sun Microsystems, famously stated in 1999 'you have zero privacy anyway, get over it' (cited in Manes, 2000, p. 312). In 2009 Google Chairman Eric Schmidt claimed that 'if you have something you don't want anyone to know then maybe you shouldn't be doing it in the first place' (quoted in Lee 2013, p. 13). While Facebook founder Mark Zuckerberg claimed in an interview that 'Having two identities for yourself is an example of a lack of integrity' (quoted in Pariser 2011, p. 109).

The technologies and services of Web 2.0 such as social networking sites (SNS), enhanced search engine capabilities and the personalised internet have shown both Zimmer (2008) and McNealy (1999) to be correct. Thus the core research question to be asked is: why is it that conceptions of privacy have changed so much within such a short space of time? Academic discussions of privacy have abounded since Warren and

Brandeis (1890) wrote about the threat posed to privacy by the burgeoning newspaper industry. Yet the reality is that despite academic and survey findings which consistently report that people are worried about losing privacy, technologies that arguably compromise it are increasingly popular. It is not just internet based technologies which can be seen to threaten privacy; as computing technology gets smaller and cheaper it becomes ubiquitous. A key element of this is the increase in digital technologies which are characterised by the fact that they leave information in their wake which can offer telling clues as to the behaviour actions and lifestyles of the data subjects. The use of such data trails as a form of surveillance has been termed 'dataveillance' (Clarke 1988). In the workplace for example, electronic key cards can be configured so that each one has a unique signature, making it possible to know exactly when each person arrives to work, how often they pass through different doors, and even how much time they spend in the bathroom. This is but one example of data generating technologies which have become unremarkable aspects of contemporary life, yet allow for the constant surveillance of people as they go about their daily routine. This research aims to explore some of the reasons for the seemingly contradictory positions relating to surveillance privacy and technology by examining the discursive repertoires used to describe them.

The first aim of this research was to enquire as to how much was known about surveillance in general. The prevailing view associates it with law enforcement and focuses primarily on visual surveillance; but the interviews aimed to enquire as to any other situations or social fields that would involve surveillance. The primary fields were those of work, consumerism and security, with each of these constituting a chapter with a brief literature review of their own. The dual aims were firstly to find out how much was known about surveillance in each situation, and secondly to find out participants opinions regarding the acceptability or otherwise of surveillance and monitoring.

The research will be presented in the following way. Chapter two will outline in more detail the research questions asked and will describe the methodological approach taken. Chapter three will be compromised of a literature review on privacy drawing on a range of historical and theoretical approaches. Chapter four will conduct a literature review on

surveillance which aims to expand the definition beyond the narrow confines of the embodied ocular gaze of law enforcement as described above. This review also draws upon a broad array of historical and theoretical approaches. Chapters five, six and seven include analysis of the interview data which has been thematically organised. Each chapter includes a brief and focussed literature review pertaining to the theme to be covered. Chapter five describes the data gathered on surveillance in the workplace, the most striking finding pertaining to surveillance and monitoring of employees was the level to which it was deemed acceptable. In the process of monitoring and keeping detailed records of work practices there emerges a sense of transparency which can be just as beneficial to employees as to management. A common complaint raised about workplace surveillance related to the monitoring of employees outside of work. The prevailing consensus among participants was that work and private life should be kept completely separate and so work life should not intrude in private life and vice-versa.

Chapter six describes surveillance in the context of security and law enforcement. A core finding here was that of a form of 'othering' of targets of surveillance; along with an almost universal recourse to the phrase 'I've got nothing to hide' which was used as a justification for not fearing certain types of surveillance. According to this logic it is those who are characterised as having something to hide who are the targets of surveillance and thus stand to lose out when it is in operation. This view creates a dualism in common consciousness between 'us' who obey the law and thus have nothing to fear, and 'them', drawn from the class of the criminal 'other'. The creation of such simplified and dichotomous identities ensures the social desirability of surveillance and serves to inoculate its proponents against meaningful discussion about the necessity, efficacy or validity of any surveillance measures. This logic also forms part of the explanation as to why systems of surveillance have spread so rapidly without much in terms of organised public opposition.

Chapter seven describes surveillance under the broad remit of consumerism, entertainment and social networking. Under these headings, the findings demonstrated

that there is a very basic understanding of surveillance, who it is conducted by, and the reasons for its occurrence. While participants mostly identified themselves as being private, their actions often left them open to surveillance in ways which they knew very little about. This was particularly evident in questions relating to consumer based surveillance, social networking and use of the internet in general. There was very little in the way of knowledge about the information economy as was most strikingly evident in the fact that most participants had no idea how either Google or Facebook make money. Chapter eight is the conclusion and discussion chapter which draws together the overall results and insights of the study.

Broadly speaking the findings were that there is a very basic understanding of surveillance, who it is conducted by, and the reasons for its occurrence. While participants mostly identified themselves as being private, their actions often left them open to surveillance in ways which they knew very little about. This was particularly evident in questions relating to consumer based surveillance, social networking and use of the internet in general. There was very little in the way of knowledge about the information economy as was most strikingly evident in the fact that most participants had no idea how either Google or Facebook make money.

Many conceptions of surveillance see it in terms of it being a top down style exercise of power, as is evident from this study it is perhaps not quite so simple. Systems of monitoring and surveillance can be seen in some instances to work both ways and in the examples of both law enforcement and work supervision; surveillance was characterised as a means of holding power to account. This means that in some limited examples subjects of surveillance are capable of reflecting its gaze back on the people or organisations conducting it.  In the case of work supervision for example, it was exhaustive systems of record keeping and oversight which made it easier for employees to hold their employers to terms of their contracts. In these terms workplace surveillance was welcomed as it allowed for greater transparency.

A further finding which related mostly to the realm of policing and security was that of a form of 'othering' of targets of surveillance. This was usually tied in with the almost ubiquitous subject position of if you have nothing to hide then you have nothing to fear. According to this logic it is those who are characterised as having something to hide who are the targets of surveillance and thus stand to lose out when it is in operation. This view creates a dualism in common consciousness between 'us' who obey the law and thus have nothing to fear, and 'them', drawn from the class of the criminal 'other'. The creation of such simplified and dichotomous identities ensures the social desirability of surveillance and serves to inoculate its proponents against meaningful discussion about the necessity or validity of any surveillance measures. This logic also forms part of the explanation as to why systems of surveillance have spread so rapidly without much in terms of organised public opposition.

# Chapter Two

# Methods

## 2.1 Quantitative or Qualitative

Surveillance and privacy are topics that have been and will continue to be widely researched across a range of disciplines. The most famous and wide reaching research into this topic is the Surveillance, Privacy and the Globalization of Personal Information International Comparisons study conducted in 2006/2007 by the Globalization of Personal Data (GPD) project at Queens University Toronto. This research undertook to 'collect data cross- nationally from a total of 9090 respondents in Brazil, Canada, China, France, Hungary, Mexico, Spain and the United States'. (Zuriek et al 2010, p. x) In the European context there are the Eurobarometer polls which are conducted across the member states of the European Union every 5 years with a sample of 27,000 respondents; these polls include questions on privacy, data protection and surveillance. Both the GPD survey and the Eurobarometer polls are conducted via the telephone, using quantitative methodologies. As these polls provide ready made and extensive data sets, there was little reason to conduct further quantitative research in this area. The knowledge gap instead pointed to the need for qualitative research that would explore the reasons behind the trends identified in both data sets. The prevailing trends identified in these studies were related to concerns of participants with losing privacy and control of their personal data. With this in mind, the interview topic guide was drawn up with close reference to the questions asked in both the GPD and Eurobarometer surveys.

To get this data from interview subjects it is preferable to allow them to speak their own words. The information garnered from quantitative research projects while useful is not capable of capturing the requisite nuances, subtleties of meaning and underlying motivations. For this reason the method that was employed in this study was the qualitative interview. Byrne (1998, p. 182) denotes the advantages of qualitative methods paying particular attention to how they are 'particularly useful as a research method for accessing individuals' attitudes and values'. The open ended nature of qualitative questioning allows for the expression of the individuals' understanding,

knowledge, experience and values in a meaningful way. As this research project aimed to ascertain the level of knowledge and understanding of people with regard to surveillance it was suited to the qualitative methodology. Bryman notes how semi-structured or flexible interview techniques are effective in comparison to structured interviews

> 'after all, if a structured method of data collection is employed, since this is bound to be the product of an investigator's ruminations about the object of enquiry, certain decisions must have been made about what he or she expects to find and about the nature of the social reality that would be encountered' (Bryman 2008, p. 389).

It was hoped that the flexible semi-structured format would open up the field of enquiry beyond the research design envisaged. In this format the participants generated areas of interest not foreseen by the researcher and were able to express the elements of the field which are of importance to them and thus worthy of further questioning and investigation.

## 2.2 Philosophy of Methods

As mentioned above; the aim of this study was to ascertain how much is known about surveillance and information gathering and its effect on conceptions of privacy. The study also aimed to uncover any discursive repertoires used by participants to explain and relate to these phenomena, and for this reason the methodology used was the semi-structured qualitative interview. This approach was by its nature subjective and interpretivist; Lazar (1998, p. 8) claims that 'the essential point of social science is to grasp *meanings* and complexes of meanings'. By attempting to situate the discursive constellations used by participants to situate the practices of surveillance, this study was attempting to decode them. In doing this it looked to an underlying subjectivist philosophy of research method. If it is the case that humans construct their own subjective worlds through the use of language and symbols; then it should be possible to

understand these worlds ontologically by analysing the ways and means by which they are constructed through language.

## 2.3 Ethical Considerations

All subjects as per agreement with the Waterford Institute of Technology Ethics Council had to be over eighteen years of age and were given an extensive fact sheet relating to the study as well as signing a detailed participation consent form (see appendices). All aspects of the study were explained including the right to withdraw, the right not to answer any question and the privacy/non-identification of all subjects. The aim of this process was to ensure that all subjects had informed consent before taking part. Informed consent 'implies that prospective research participants should be given as much information as might be needed to make an informed decision about whether or not they wish to participate in a study' (Bryman 694, p. 2008).

## 2.4 Sampling and Gaining Access

As per the terms of the WIT ethics committee all participants had to be over eighteen years of age, aside from this stipulation the sample was as broad as possible. The sample aimed to be as broadly representative of the Irish population as possible but with slightly more males than females and as good a match of the age ranges as is possible. The sample group consisted of fifteen people, each of whom took part in an interview which lasted between sixty and ninety minutes. Of the fifteen people interviewed, seven were male and eight were female, with a mean age of thirty. The youngest participant was nineteen years old, and the oldest was forty-six.

In order to gain access to subjects a number of methods were employed, the first method involved recruiting through word of mouth. This involved asking friends, acquaintances and colleagues to nominate people known to them but not to the researcher. This method was used for the early trial run interviews and yielded a return of five participants. These trial run interviews were particularly useful as means of honing and refining the interview techniques and questions and ruling out questions or

vignettes that did not yield useful data. The next level of recruitment came through the process of snowballing, at the end of each interview the subject was asked to recommend any other people who might be suitable for interview. This process yielded a further four participants and was useful for gaining access to particular social and age groups. During the course of the research social networking websites were also utilised as a way of spreading word of mouth and of contacting people recommended during the snowballing exercise. Social networking played a vital role in recruitment, in the second year of the project a Facebook group was set up for recruitment purposes. This group however grew from this function to being an online space where members could talk about issues relating to the research. The group page was also used to highlight media stories that were related to aspects of the research, these included the News of the World Phone Hacking Scandal, the British Governmental response to the London riots of August 2011 and the use of Data Matching techniques by various departments of the Irish State among others. This meant that conversation and debate was stoked among members of the group which had a further effect of drawing in more members which in turn led to more interview subjects. The number of people recruited through online social networking was limited however so as to avoid the narrowing of the sample to people who use such sites. In order to recruit older and non online social network using participants a number of other methods were used. An offline social network was tapped into through a pub; after a couple of patrons of a particular pub were interviewed other patrons became curious and sought out the researcher so as to participate. This yielded a very small number of participants but did include a number of people who would not have been reached via the internet. A further group was contacted through Vocational Educational Colleges in Wexford and Waterford, administrators were contacted via email and then with a follow up call which introduced the researcher and the research. This method however did not yield significant results and no participants were recruited in this fashion.

There was a reasonably broad range of professions included within the sample; the method of classification used was NACE which is the standard mode of classification used by both the CSO and the EU. NACE stands for ‘Nomenclature générale des

Activités économiques dans le Communautés Européennes; since its introduction in the 1970's NACE has been revised a number of times; the version currently in use is NACE rev 2 which classifies economic activity under headings ranging from A to U. Immediately four participants are outside of the NACE system as two were unemployed and a further two were in third level education. Instead of receiving the A to U assignation relating to their profession, these participants were marked N/A. The table below lists the participants under the headings of name, age, gender and profession. For the purpose of maintaining the anonymity of participants the names listed here have been changed. For the same reason the listings under profession have been included in the broader NACE categories.

| **Name** | **Age** | **Gender** | **Profession** |
|---|---|---|---|
| Peter | 35 | Male | Transportation and Storage (H) |
| Carol | 19 | Female | Student (N/A) |
| Darren | 33 | Male | Education (P) |
| Anna | 27 | Female | Wholesale and Retail Trade (G) |
| Sean | 48 | Male | Human Health and Social Work Activities (Q) |
| Margaret | 43 | Female | Human Health and Social Work Activities (Q) |
| Paul | 31 | Male | Unemployed (N/A) |
| Hannah | 38 | Female | Financial and Insurance Activities (K) |
| Pat | 38 | Male | Information and Communication (J) |
| Mary | 22 | Female | Wholesale and Retail Trade (G) |
| Harry | 31 | Male | Unemployed (N/A) |
| Amy | 20 | Female | Student (N/A) |
| Rory | 23 | Male | Wholesale and Retail Trade (G) |
| Jane | 19 | Female | Wholesale and Retail Trade (G) |
| Brid | 23 | Female | Accommodation and Food Service Activities (I) |

## 2.5 Potential Impediments

Before conducting interviews it was necessary to consider all factors which could potentially have had a distorting effect on the results 'These will include who is doing the interviewing, who is being interviewed, the location in which the interview takes place and the form of questioning' (Byrne 1998, p. 180). As part of the research design all of these questions were considered so as to offset as much as possible the likelihood of distortion, misrepresentation or bias. All interviews were carried out by the researcher and in order to minimise the potential for leading any subjects, and with the express intention of minimising or eradicating confirmation bias, the interviewer did not express any sentiments of approval or disapproval towards any opinion on the subject. The research design strived towards a neutral line of questioning so as to minimise bias built into the language of the questions.

With each participant the location of the interview was designated as a place of their choosing, this was predominantly either in the participant's home or in a neutral location such as a hotel, coffee shop or pub. The only real stipulation was that the location be quiet enough to allow for the recording of decipherable audio. The style of the interview was determinedly informal with every effort being made to make the subjects at ease and comfortable. The interview itself followed a semi-structured template, there was a list of topics and questions to be covered but the order in which they were discussed was determined by the flow of the conversation. While this structure allowed for a conversational style which put respondents at ease, having a set list of themes, topics and questions made it easier to compare the answers of different respondents and to thematically categorise and analyze them at a later stage

## 2.6 Composing the Questions

As mentioned above, the GPD and Eurobarometer surveys offer a solid foundation in this area of research, thus they were the first points of reference when composing the questions. The topics in consideration aimed to cover the variety of social roles where surveillance is common; these include the roles of worker, traveller, citizen and

consumer. As the aim was to be as informal and casual as possible each role was brought up with open ended lead in questions such as ‘so tell me about the last place you worked in’. In this instance once the respondent was talking about their workplace it was then possible to introduce questions relating to levels of surveillance and monitoring that accompany their work.

The interview started with a short list of surveillance technologies being read out and the respondent being asked if they were familiar with any of them. The list was comprised of: Closed Circuit Television (CCTV), Biometrics, Data Mining, Data Matching, Automatic Number Plate Recognition (ANPR), Facial Recognition Systems, Global Positioning Systems (GPS), Cookies, and Radio Frequency Identification Tags (RFID). By starting with such a list it was possible to gauge early on in the interview how much was known about each technology, it also opened up the discussion by asking where the technology is used. The form that the remainder of the interview took depended on the response given to the opening questions; if the respondent showed any knowledge of a particular technology or site of surveillance, then the line of questioning followed this knowledge. In cases where the respondent was unfamiliar with any of the technologies of surveillance broader questions regarding the nature of privacy and surveillance were asked.

As a further means of getting respondents to think about technologically mediated surveillance a question was raised which asked them to describe a typical day and list any activities that leave a digital footprint. The concept of a digital footprint was explained by reference to the commonly conceived idea of a carbon footprint. By explaining it this way all respondents understood exactly what was being asked and were able to describe a typical day while denoting any perceived interfaces between themselves and technology which left a digital trace. Activities that were described included among others shopping, internet activity, working, driving, and using mobile telephones.

In covering the broad topic of Surveillance, the discussion began by asking ‘what do you understand surveillance to mean?’ Once an answer was given the next question asked, ‘can you think of any instance where you would be under surveillance?’ The first question is quite open ended and allows for further clarification and probing, while the second question is not open ended it was possible when the respondent simply answered ‘no’ to clarify the question and give an example of potential surveillance based on social roles. Once these questions were answered and an understanding of what surveillance is and where it is in operation was reached, the final section related to how the respondent feels about being under surveillance. In particular it was hoped to find out if people had given any thought to the various systems which monitor them in their everyday lives.

A similar line of questioning was utilised with the aim of addressing the matter of how respondents view privacy. This section started by asking ‘what do you understand privacy to be? Once again the follow on questions were determined by the answer given but in general the follow on questions would ask the respondent how important they think privacy is, what aspects of their life should be kept private, and whether or not we have less privacy now than we did in the past.

A further line of questioning related to methods of resisting or subverting surveillance. The opening question asked ‘have you ever deliberately withheld or given false or misleading information to an organisation because you felt that the information requested was unnecessary’? The Globalisation of Personal Data survey asked similar questions with the intention of finding out the extent to which people alter their behaviour so as to protect themselves from unnecessary intrusion and to protect their personal information. Included in this rubric of resistance would be everything from using a pseudonym, giving a different address to withholding any form of information which would allow for identification among others.

## 2.7 Vignettes

There can be a problem of definition when asking questions about topics such as surveillance and privacy. Surveillance and privacy are both value laden terms which have an inbuilt set of assumptions; these include the assumption that surveillance is bad, authoritarian and intrusive and the assumption that privacy is good and must always be protected at all costs. The conversational nature of qualitative semi-structured interviews allows the interviewer to clearly define such terms; but this process still cannot fully remove the residual values associated with the terminology. The terms of definition are also important as for example the word privacy can be said to have many distinct meanings including secrecy, freedom from outside observation/interference and the control over personal information flows. With terms having such variance of meaning it is not always possible to determine which sense of the word the interviewee is using. Both of these problems show a weakness in the method of asking questions on seemingly abstract concepts.

A means of addressing these problems was through the use of content specific vignettes; this method involved the construction of brief third person narratives which give examples of the concepts in question. Hughes describes vignettes as being 'stories about individuals, situations and structures which can make reference to important points in the perceptions, beliefs and attitudes' (1998, p. 381). After the vignette was read the respondents' opinion was sought about potential issues raised. According to Pavlov 'respondents are less likely to be biased in their responses if given a standardized, contextualized situation in which they are asked to give their views regarding the behaviour of neutral persons other than themselves '(Pavlov 2008, p. 31). Thus vignettes offered an applied real world example of the concept in question while the use of a third person narrative gave the respondents a level of distance from themselves which could potentially allow for more honest answers. At the point of analysis the vignettes also offered an opportunity to explore the differences between self declaration and third person declaration. Self declaration refers to the respondent's answers to questions asked

directly of them, for example what is your opinion on Garda traffic surveillance? Third person declaration refers to the answers given to the questions relating to the vignettes.

In drawing up the vignettes to be used there were a number of factors which had to be considered. Stories must be believable and describe everyday situations and must avoid describing exceptional situations, circumstances or characters. In using content specific vignettes the aim was to describe mundane, believable and relatable situations and characters (Barter and Renold 1999, p. 3) (Finch 1987, p. 107) (Veal 2002, p. 2). A further element of consideration was that of the length and complexity of the vignette; Finch (1987, p. 107) claims that more than three changes to a storyline in a vignette will render it too complex and difficult for respondents to remember. With this in mind the vignettes used were short, concise and to the point.

In framing the vignettes two social roles were used; namely traveller/motorist, and shopper/consumer. In the case of traveller/motorist the vignette used is as follows:

> 'Sean left home to go to work, as he drove towards town he passed a Garda traffic corps car which recorded his registration, his car tax situation, the direction he was travelling and the time'

This vignette describes the workings of the Garda automatic number plate recognition (ANPR) system which is mentioned among the first question in the interview. As mentioned above, Barter and Renold advise that stories should avoid unusual or exceptional circumstances. In the first vignette the fact that Sean is driving to work aimed to present him as an everyday working person and thus contextually place him as a law abiding and hard working person. After reading this vignette the respondent was asked whether Sean's privacy had been respected and this was the lead in question to start a discussion on the role of surveillance in law enforcement. By anchoring the question on a third party it was possible to ask questions again that were asked earlier, although the second time around the answer was based on a fictional third party and thus

there was a level of subjective distanciation where the respondent was not answering about themselves and as such could potentially give more honest answers.

The next two vignettes were based around consumer surveillance, the first is as follows:

> 'Mary was shopping on the internet for a new pair of shoes, she went to site a.com and found a pair she liked, later she found and bought the same shoes at a lower price on site b.com. When Mary went on to site a, her activity on the site was tracked for marketing purposes, a report was compiled which showed what items Mary had looked at, how long she looked at them, and which site she ultimately used to purchase her shoes.'

Again the name Mary is a typical Irish name, the vignette was again followed by the question has Mary's privacy been respected? In this instance this was a lead in question to start a conversation on consumer surveillance in the context of a third party. The final vignette is also based on consumer surveillance:

> 'Ann shops regularly in the same supermarket, she recently accepted a loyalty points card which she presents at the till each time she is shopping. By using the card she gets a discount on her purchases, in return for this the supermarket gets a detailed list of her preferences and they can compile a profile of their customers. The information held by the supermarket is then sold on to other marketing companies.'

Once more the question of privacy was asked, in this instance it is as a lead in question to start a conversation on customer profiling and consumer surveillance. A further vignette which was based on real life experience used in the early trial run interviews. The story was taken from the Data Protection Commissioner (DPC) website and it described an instance of data being gathered for one purpose and used without permission for another. In the trial run interviews the story did not seem to work as a

means of starting a broader conversation and for this reason it was not included in the final interview guide.

### 2.8 Data Analysis

After conducting the interviews, the audio files were securely stored on a recording device, a private password protected computer and on a password protected flash drive memory stick. After listening back to the interviews it was decided that eleven of them had high quality usable content and these interviews were transcribed in full. Minor aspects of the remaining four interviews were written up, but the vast majority of the content to be analysed was taken from the eleven transcribed interviews. The transcripts were loaded into the NVIVO text editing program and were coded according to content. The preliminary coding involved gathering answers to each question and organising them thematically. The themes included the use of common phrases or responses such as 'I've got nothing to hide', every time this phrase occurred was marked and assigned to a node in the NVIVO program. This allowed for an overview of instances of its usage and allowed for it to be contextualised. As well as making nodes based on phrases; there were nodes based on each theme and the different reactions to them. This lead to nodes such as 'workplace monitoring, positive' which would denote an instance where a participant mentioned an instance of workplace surveillance and described it using positive terms. Using such nodes allowed for the large data set to be organised into coherent blocks which allowed for more robust analysis. The process of editing and content coding the text files was thus instrumental in spotting the trends and themes which had emerged from the data gathering stage.

### 2.9 Discursive Repertoires

The data gathered at the interview stage was subjected to discourse analysis with the aim of uncovering and elucidating any discursive repertoires. These are 'lexicons of linguistic resources used by individuals in their accounts' (Ball and Wilson 2000, p. 544) to shape the meaning and understanding of a given topic. Discourse analysis 'emphasizes the role of language as a power resource that is related to ideology and socio-cultural change,' (Bryman 2008, p. 508) discourse analysis uses language- written

or spoken- as the object of investigation and aims to discover the social structures, and processes behind the use of language and the generation of subjective meaning In the context of surveillance and computer based monitoring and retention of personal data there are a number of predominant discursive repertoires. One is ‘if you have nothing to hide then you have nothing to fear’. This statement has been analyzed and discussed at length by Daniel Solove (2004, 2007, 2011) and O’Hara and Shadbolt (2008) among others and will be looked at in detail in the discussion chapter. During the process of analysis of interview content further discursive repertoires were uncovered relating to conceptions of privacy and surveillance which reveal the discursive constructions of meaning; these repertoires will also be examined in the conclusion and discussion chapter.

# Chapter Three

## Privacy

'Privacy, like the weather, is much discussed, little understood and difficult to control' (Gary T. Marx quoted in Ritzer 2007)

'I think judgement matters. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.'
(Google CEO Eric Schmidt CNBC interview 2010 )

### 3.1 Introduction

Privacy has become one of the primary battlegrounds of the information age; in the media and general public discourse it is commonly held as the antithesis to surveillance; or as something which must be relinquished to adequately facilitate public safety and security. A problem arises at the outset however as there is confusion as to what exactly privacy is. To define privacy is a notoriously difficult task; the Penguin dictionary (2002) describes it as 'a state of being apart from the company or observation of others, freedom from undesirable intrusions *esp* avoidance of publicity'. This definition is overly individualistic and describes just one aspect of privacy namely seclusion; in these terms privacy is essentially formulated as the Warren and Brandeis 'right to be left alone' (1890, p. 2). Conceptualising privacy is fraught with difficulties due to the fact that traditional definitions and commonly held assumptions about it have been rendered problematic in the face of technological advances and changing socio-cultural norms about what constitutes the public and the private. The depth and variety of privacy theory spans across multiple disciplines such as philosophy, psychology, legal studies, computer science and sociology. Limits of space mean that the full spectrum of perspectives on privacy will not be accounted for here; instead some of the sociological and psychological perspectives will be examined in an attempt to paint a broad brush strokes picture of what privacy is.

The socio-cultural changes relating to privacy will be looked at with close reference to Norbert Elias and the civilising process with a particular emphasis on the changing nature of space, particularly in the household. The aim of this is to define privacy as an inherently social value by emphasising the changing parameters used to delineate the private or individual spaces. This will be followed by an examination of the traditional conception of privacy which is rooted in liberal-individualist thought and emphasises the primacy of the rights of the individual. This individualist view will then be interrogated with reference to Etzioni (1999) and the communitarian approach, as well as more contemporary and social conceptions of privacy such as Steeves (2003) and Nissenbaum (2010). The aim of this is to explain privacy as an important and necessary 'social good' (Kasper 2007, p.165) and so to show its importance not just to individuals but to societies at large. The limitations of privacy with respect to it's being an antidote to surveillance will be looked at with reference to Lyon (2007) and Stalder (2002, p.120) as well as the limitations of privacy as a 'discourse of rights' (Gilliom 2001, p.120). The thread which will run through this argument is the assertion that privacy is not a selfish or individualist concept and is in fact is a core element of any functioning society as it is central to processes of identity formation and socialisation. As well as this it will be shown that privacy is an ever changing concept which makes it difficult for it to be utilised as the sole panacea for surveillance.

### 3.2 Historical Context

As a means of placing privacy in an historical perspective; the writings of Norbert Elias and the civilising process will be discussed first. As will be shown below, privacy is an inherently social value and the origins of this value can be described with particular attention being paid to the evolution of privacy with reference to manners and social space. Contemporary social sensibilities posit a strict separation of domestic space related to functions; for example the kitchen is where food is prepared, the bedroom where a person sleeps and the sitting room is where guests or visitors are entertained. In this sense the bedroom and the bathroom are essentially private spaces, the bodily functions or bathroom acts are carried out behind the scenes of social life and the bedroom is a private space which is generally not open to visitors. This schema of public and private spaces within the home however is not fixed and nor has it always been, in

fact the socio-cultural norms regarding domestic space have changed considerably over time. The changing of functions came about primarily due to rising economic and living standards and changes in manners and socially acceptable behaviour, these changes occurred as part of what Elias called the civilising process. By examining etiquette and manners books from the Middle Ages onwards Elias was able to ascertain how much standards have changed. Included amongst these changes were those evident in standards of manners and domestic arrangements.

With regard to the utilisation of domestic space much has changed, 'in medieval society…. People were received in bedrooms, even from the bed. It was common for many people to spend the night in the same room' (Mennell 1992, p. 40). Indeed this fact of people sharing beds is also apparent in The Canterbury Tales, written by Chaucer in the 14th Century where many of the pilgrims shared a large bed when stopping overnight at the Tabard Inn tavern. This shows that the current delineation of the status of the bedroom as a private space has evolved and is not in any sense constant. Changes like this are also apparent if past norms regarding toilet behaviour and bathing are compared with those of the present. In the case of bathing, this was a communal activity in the middle ages, the bathing houses which were popular were communal and being naked around others was commonplace (Mennell 1992, p. 41). In the case of toilet behaviour it was not seen as unusual to talk about it until around the 18th Century and 'as late as 1589 the Brunswick Court regulations decree: 'let no-one, whoever he may be, before, at, or after meals, early or late, foul the staircases, corridors or closets with urine or other filth but go to suitable prescribed places for such relief' (Mennell 1992, p. 39). As the use of such prescribed places became commonplace the acts themselves slowly became 'invested with feelings of shame and repugnance' (Mennell 1992, p. 39) and this meant that toilet usage was pushed further and further back behind the scenes of social life and thus into the realm of the completely private.

While the evolution of manners and etiquette may not on the face of it have much to do with privacy; the changing of social spaces from public to private is worth remarking upon. The move towards private individualised spaces for bathing, sleeping and toilet

activities is also apparent in the change from communal dishes and patterns of eating to the more individualised and present forms. This movement from the communal and shared to the individual and private has led to the development of 'the invisible wall of affects which seems now to arise between one human body and another, repelling and separating' (Elias (1939) 1994, p. 69).

The movement from communal to individual is also evident if changes in social housing are considered. 'The bathroom and the bedroom in all but lower class homes, are places from which the downstairs audience are excluded' (Goffman 1956, p. 123). If the standards for social housing in the 1900's are compared to that of the present day; these changes become clear. The slum dwellings of the early 20th century housed more than one family in the building with there often being even more than one family per room. In contemporary social housing one family –generally of a much smaller size- would occupy a whole house which would most often consist of three bedrooms. This long term process of individualisation with respect to space is arguably continuing to the present as family homes are divided up and children are allocated their own spaces to watch television or play separately from the adults.

### 3.3 Privacy and the Latitude to Lie

A common critique of privacy states the view that it is merely a veil behind which dishonest, immoral or illegal deeds can be carried out, this view is typified by the quote at the top from Eric Schmidt. In this sense privacy is not a socially desirable trait and most certainly should not be afforded the status of an individual right. It is instead a hiding place for recalcitrant wrong doers who use it to disguise and facilitate their duplicitous illegal and immoral activities. Privacy in this sense is equated with secrecy and deceit which in turn are equated with deception. Deception can be carried out for a number of reasons varying from telling a white lie to avoid hurting someone's feelings up to deceiving others in a criminal sense for financial gain. In looking at privacy in this way the first question asked is what is it that people who look for privacy are hiding, as privacy affords individuals with the 'latitude to lie' (Depaulo et al 2003, p. 397).

When a person has distinct and discrete roles or interactions; they also have more opportunities for deception and the latitude to lie. The relation of this dynamic to selfhood and privacy will be discussed below with reference to Goffman (1961) and total institutions, but this equation of privacy with deception can be illustrated in some of the various confidence tricks that have been perpetrated in the past. DePaulo et al. (2003, p. 401) cite the example of 'the count' Lustig who sold the Eiffel Tower to scrap dealers by posing as a government minister. Similar methods of deception are commonly found online in the various types of 'advance fee fraud' (Yar 2006, p. 85) such as the Nigerian Letter Scam or the Spanish Prisoner. These frauds offer what seems to be privileged insider information, in the Nigerian Letter scam it is that there is a sizable amount of money which needs to be released from a Nigerian bank. The mail purports to come from an ex-politician and the letter explicitly or implicitly states that the funds are ill-gotten often through political corruption and because of this need to be accessed by someone who is not connected to the political system. By giving such information the perpetrators are attempting to form a bond with their targets through the dissemination of private or secret information. This willingness to give over such information does gain the trust of some as they are complicit in an illicit transaction. According to Yar (2006, p. 87) the average amount scammed in each instance of this fraud is 3000 US dollars although it is almost impossible to know how many instances of this type of fraud have occurred because of underreporting. This is because the fraud is designed to make the target complicit in wrongdoing and thus less likely to report it. By using privacy and alleged insider information the conman not only gains the trust of the target but also isolates him so that after the fraud has been committed the victim 'keeps his victimisation to himself in order to save face' (DePaulo et al 2003, p. 402). This is but one example of how privacy can be used to facilitate deception.

### 3.4 Nothing to Hide?

The most common form of rebuttal to calls for privacy is found in the ever present maxim of if you have nothing to hide then you have nothing to fear. This logic has it that it is only those who have committed or are continually committing crimes or misdeeds that should be worried about diminishing privacy or increasing surveillance. This logic

creates a clear line of cleavage between right and wrong, it creates a verisimilitude of transparency or openness with good, and privacy with bad. The identification of those who are good is thus underlined and emphasised by their willingness to be transparent, to show any requested details of their life to relevant people or authorities. This logic also extends to render any form of privacy problematic by equating it with wrongdoing; if it is the case that surveillance uncovers wrongdoing then the person has no claim to privacy anyway because of that wrongdoing (Solove 2008, p. 746). A further strand to the argument is clear when people claim that they don't break any laws or do anything that could place them under suspicion and so they don't mind having their activities tracked or monitored. Due to the prevalence of the nothing to hide argument in both public discussions and the interviews there will be a distinct section in the conclusion chapter which will discuss it at length.

### 3.5 Defining Privacy

As has been shown above the idea of what constitutes private space is in constant flux, as is the concept of privacy itself. If asked to define privacy the most common response given is that which relates to personal and private space. 'Its walls are bulwarks against external intruders … the private sphere keeps others at a distance and provides a person with a secure place in the world' (Sofsky 2007, p. 30). This spatial metaphor which sees privacy as being a space or bubble which must be protected against encroachment is limited. This is because the 'bubble' of privacy is progressively contracting as technological advances bring more and more digital technology into the realms of the family, entertainment and social life. 'The information revolution has implanted zones of publicity into the once private interior spaces of the self and home' (Sheller and Urry 2003, p. 122). This spatial definition of privacy is closely bound with language where privacy is spoken of as being 'invaded' by an outside entity. Yet this metaphorical and linguistic use stems from older definitions which were based on the conceptual and legal sanctity of the home as a private space which was free from outside intervention and monitoring.

In exploring some of these older definitions the starting point is one of the most often quoted which is Warren and Brandeis who define privacy quite simply as 'the right to be left alone' (Warren and Brandeis 1890 p 1). In formulating this definition the authors had in mind the protection of individuals from the new technology of photography and the nascent newspaper industry.

> 'Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops' (Warren and Brandeis 1890, p. 2).

At the time of writing in 19th Century America, Warren and Brandeis were attempting to further regulate the potential of the press to cause damage to the individual. While there were various slander and libel laws in place, they were confined to the damage done to a person in his or her external relations with society and reputation and its protection was central to these laws. There were no laws which dealt with damage inflicted on an individuals' sense of self worth or self estimation and it was such 'injury to the feelings' (Warren and Brandeis 1890, p. 2) that the authors were writing to correct. This definition of privacy is often quoted but in practical terms is very limited as the authors did not aim to definitively state what privacy was and instead aimed to legislate in common law a right to privacy.

Such a simple definition raises many questions, the parameters of what constitutes privacy are vague, it makes no mention of how, where or when a person has the right to be left alone. In this sense privacy can be seen in terms of opposition, it is a zero sum game where the individual is pitted against society at large and any claim to individual privacy is made against the claims of society such as security or efficiency. This version of privacy is based on liberal-individualist thought which has its roots in the writings of John Stuart Mill on Liberty which discusses the nature of the relationship between the individual and society. It invokes the private individual who is free from interference from the state and from others as long as the individual is not causing direct harm to

anyone else. It stresses the primacy of the individual and places his or her rights above those of the community. In the broadest sense of this definition privacy is essentially isolation from others; ‘solitude is the most complete state of privacy that individuals can achieve’ (Westin 1967, p. 7) so privacy thus defined is lost once one enters social relations. Nissenbaum describes as being unhelpful, a definition of privacy that is described ‘in such a way that it is violated every time a motorist peers at a pedestrian crossing the street’ (Nissenbaum 2010, p. 73).

Alan Westin describes privacy as ‘the claim of individuals groups or institutions to determine for themselves when, how and to what extent information about them is viewed by others’ (Westin 1967, p. 7). This type of privacy is based around the concept of limited access to the self; it is concerned with the individual being able to control who has access to them, when, and under what circumstances. This definition was instrumental in the formation of various international data protection laws as it is focused on data. Westin was among the first to theorise privacy in definitional terms, his most lasting contribution was his description of the four states and functions of privacy. Each state or condition of privacy is matched by a function which shows its reason or importance. The first state of privacy is solitude, this describes spatial separation from other people which means that others cannot observe or listen. By being in a state of solitude it is possible for a person to avoid being influenced, dominated exposed or manipulated by others, so the corresponding function of solitude is personal autonomy.

The Second state of privacy is intimacy; this state is similar to Goffman’s (1959, p. 24) writings on backstage areas which will be looked at in further detail below. Intimacy relates to the seclusion of a small group of confidantes or trusted others. The function of intimacy is to allow for the formation of emotionally significant relationships which are free from the expectations of social roles, conventions, or expectations in the social world at large. The state of intimacy allows for people to be honest and open and provides a resting place from the demands of social life. Anonymity is the third state of privacy; this relates to the freedom of the individual from identification and surveillance in public spaces, this state of privacy allows for self evaluation and freedom of

movement. Westins fourth state of privacy is reserve which is based on the ability of people to limit disclosures about themselves. By having the power to limit what is known about them, people have the ability to limit and protect the information relating to them. In having this capability, people are able to restrict any information about them that is unflattering or damaging to their reputation. Westin refers to this as the function of limited and protected communication and this function is integral for social identification purposes; people can use this function to present themselves in a manner befitting the situation through the limiting of some information about them and the displaying of others.

Westins states of privacy are solitude, intimacy, anonymity and limited and protected communication. While this attempt at creating an operational definition of privacy is laudable, it is the case that this definition is overly individualist. While Westin makes reference to the need to balance the needs of the society with that of the individual he does not make much of the social side of the equation. While he drew on social elements in his theory of privacy drawing on Goffman and Simmell; the states of privacy are described almost exclusively in terms of their efficacy and utility to the individual. Westin's formulation of privacy while seminal has been criticised for this reason by Regan (1995) Steeves (2003), Stalder (2002) and Andrejevic (2002). A further mode of criticism relates to how this definition which has informed the various international data protection regimes is too heavily focused on the control of information. This focus has not stemmed the multitude of flows of personal information towards and from institutions and corporations.

While the value of privacy to the individual is aptly described by Westin; a communitarian critique of this view can be found in Etzioni in his 1999 book The Limits of Privacy. Etzioni describes privacy as 'an individual right that is to be balanced with concerns for the common good' (1999, p. 4). In the process of balancing, privacy is seen as just one right or good which is not 'privileged' above any others. This idea of privacy as a right which must be balanced against others is found in both Irish and European laws on Privacy. Each individual right must be balanced not just against other individual

rights but also against wider social responsibilities. If this happens then the primacy of privacy as an overly individualistic right will be adequately countered. The communitarian approach to privacy is important as it places it amongst other competing rights and responsibilities, but this approach does not adequately describe the social value of privacy.

### 3.6 Privacy as a Social Value

The need for a social perspective on privacy is succinctly stated by Barrington Moore who claims that 'the need for privacy is a socially created need, without society there would be no need for privacy' (1984, p. 73). The definitions of privacy examined so far have focussed on how it affects individuals; a further strand of the concept is to be found if one looks at the social values and benefits of privacy. The social aspects of privacy as it relates to the individual have been discussed above, the importance of privacy as a social good for society itself will now be discussed with particular reference to Steeves (2003) Regan (1995) and Nissenbaum (1998 )(2010). The liberal individualist view of privacy described above is always likely to be subordinate to other social values. If privacy is claimed and defined as an *individual* right, then *social* rights or needs such as freedom of speech or the press, health, security, prosperity, and efficiency will win out each time. In keeping with the communitarian view described above, the individual rights of privacy will be trumped by the collective responsibilities when the process of balancing is undertaken. Privacy needs then to be taken out of the realm of individualism and placed into a social context which shows its necessity in functioning societies. In order to do this it is necessary to reference role theory, particularly Erving Goffman.

In his study of the interaction order of social life Erving Goffman devised a scheme based around a dramaturgical metaphor. This scheme viewed social life in terms of 'performances' (1959, p. 15) where people present themselves in particular ways depending on the situation. The dramaturgical metaphor was further utilised when describing front and back areas. 'Front areas' (1959, p. 22) are those where a performance must be maintained such as in a restaurant; when waiting staff are in view of customers they must maintain the decorum, the manners, the gait and any other relevant behaviours associated with the 'performance' of being a waiter. Back areas then

describe the places where the staff are out of sight of the customers and so can drop the behaviours associated with the performance. In a wider sense if social life is divided up into front and back areas then to some degree almost all areas involve some element of performance which is determined by the situation and the roles associated with it. In the sense of privacy then, a Goffmanian perspective would determine the home as being an inviolable space where the performances of social life at large can be dropped and the essential or true self can be revealed. Richard Jenkins describes back areas as places where people can 'be free of the anxieties of presentation, it is the domain of self image rather than public image' (Jenkins 2004, p.71). In this sense then privacy is the domain of self development, a place free from the necessities of maintaining public performances or faces, a place where one can be their true self. In this vein DePaulo et al describe backstage areas as a place where 'we can exchange the costumes we donned to draw an admiring crowd for our shabby old jammies' (2003, p. 397). At the level of the individual Westin draws on Robert Park and claims that this ability to withdraw to the realm of the private allows for 'reflective solitude' which allows for an organisation of the self which enables the individual to 'integrate his experiences into a meaningful pattern and to exert his individuality on events' (Westin 1967 cited in Steeves 2009, p. 198). This reflective solitude also allows for intellectual development as people can take time out from social interaction. In the space free of the necessity of social performance afforded by privacy; they can relive past interactions, imagine those which could happen in the future and rehearse. 'Privacy is central to one's development of autonomy, problem solving skills and communicative capacity. We use private time to organize our interpretations about daily thoughts, behaviours, and our place in society' (Kaspers 2007, p. 173).

In the sense of backstage areas there is not just the benefit accrued to individuals, but for similar reasons there are benefits for society as a whole. If individuals are given the space and time for personal development and self reflexivity, then society will benefit from being constituted by more rounded individuals. While Westin defined the fullest state of privacy in terms of withdrawal from sociality; Irwin Altman defined privacy as 'a dynamic process involving selective control over a self-boundary' (1975, p. 6). It is

through the continued process of engagement and withdrawal from sociality that boundaries between people are maintained and social identities are created based on these boundaries and markers of difference. As well as privacy being a space for self creation and development which benefits society at large; it is also a space which fosters group solidarity. In the back areas mentioned above when discussing Goffman there was mention of a true self free from the necessity of masks which are dictated by social roles. In this back space strong ties are formed and maintained such as in the family unit where inhibitions can be lowered and confidences earned and maintained. These sorts of ties thus form the bedrock of social bonding and solidarity.

Social interaction requires brief periods or spaces of privacy which can be used to manage performances. It is never the case that a person is fully and truly known by those around them, that all of their thoughts and intentions are clear. Instead people interact with each other by the selective revelation of parts of themselves or what they are thinking and the retention of others. This allows for people to avoid social awkwardness, embarrassment or insult to others, and to fit into the given social situation. This is a further example of the process of engagement and withdrawal described by Altman (1975, p. 6), and more presciently Goffman. In Asylums (1959) Goffman described 'total institutions' such as prisons or mental hospitals where 'all aspects of life are conducted in the same place and under the same single authority' (Goffman 1959, p.6). This brings about 'role dispossession' (Goffman 1959, p.14) as the compression of authority and space in total institutions means that it is not possible for inmates to alter performances or roles, as they are constantly held to account by the staff of the institution. Outside of total institutions the segregation of roles, situations and the audience who receives them means that there is a variety of spaces, roles, and behaviours which individuals can act out in isolation from each other in what Goffman terms 'role scheduling'(Goffman 1959, p. 14). In the total institution 'spheres of life are desegregated, so that an inmates conduct in one scene of activity is thrown up to him by staff as a comment and check upon his conduct in another context' (Goffman 1959, p. 36). The total institution is a manifestation of a situation where inmates are denied privacy and as such is a useful concept for exploring its importance. One of the key

features of total institutions regarding their inmates is the aim of 'curtailment of the self' (Goffman 1959, p. 46), by breaking down inmates social identities, sense of agency, autonomy, and general selfhood; the institution can remould the inmate to fit in with given institutional prerogatives. This shows the centrality and importance of private space and reflective solitude to the creation and maintenance of selfhood.

This account is a bottom up description of living under constant surveillance where all 'performances' or 'masks' are tied to the individual. Interestingly this holding to account through constant visibility has manifested itself at the highest levels of power, namely interstate relations. The need for privacy in diplomatic circles has been highlighted by the Wikileaks affair, where supposedly secret diplomatic cables were leaked to the public much to the embarrassment of many diplomatic and political actors. The need for presentation management, or the ability of diplomats to speak to their home countries in confidence while presenting a face to their host country is emblematic of the necessity in wider social interaction for telling white lies withholding certain information, or generally tailoring a performance to the audience who is receiving it. The use of privacy as a means of facilitating impression management is one of the cornerstones of social interactionism.

### 3.7 Privacy and Social Stratification

Privacy in a social sense is also something that is associated with stratification and social class. In some ways it can be described in terms of it being an asset that can be bought; the simplest formulation being that the more money a person has the more they can afford privacy. This is most obviously apparent in housing where privacy is a tangible asset which can positively affect the market value of a house. The wealthy can afford to live in homes which are private; they can afford to live where nobody can watch them or where they can control who has access to them. The larger a house is the more there is room for individualised private spaces for each of its inhabitants. Privacy and the control of access with respect to housing is also apparent in the phenomena of gated communities; where for a price people can live in estates which are enclosed and protected by CCTV and security operatives who closely monitor the space. While it

could be argued that describing such a monitored space as private is paradoxical; it must be pointed out that such communities are monitored solely for the purpose of the security of its inhabitants. People are checked on entry and exit, and only those who 'belong' are allowed in, the monitoring and fencing of such communities is essentially an embodied architectural form of limited access to the self. The purpose is to differentiate between those who belong and those who don't and to repel and expel the latter to facilitate the safety of the former.

Those who hold the resources can also buy privacy in other technological forms such as privacy enhancing technologies (PET's) which can be used online to cloak internet activity or to encode internet communication. While financial resources allow for this, it is also the case that the higher up the social scale we go, the more likely we are to find people with other forms of cultural capital such as education or technical knowledge. It is people with education who are more likely to know about and know how to operate privacy enhancing technologies and know about their legal rights. It is also worth considering the focus of authority when considering stratification and privacy. In the operation of CCTV it is usually the case that the targets of surveillance will be young working class males. As well as being targeted by surveillance these people are more likely to come in contact with the police in 'stop and search' actions and other random checks which occur as part of the process of what Marx terms 'categorical suspicion' (1988, p. 219). This is where people who belong to categories deemed suspect are singled out for special treatment such as increased surveillance or a higher level of Police attention. It is only due to their imputed belonging to such categories that such treatment occurs; meaning that many who have committed no crime will be the focus of police attention due to such discriminatory practices. Poorer people will comparatively lack resources financial or cultural which will allow them gain the same level of privacy as those above them in the social scale; this means that privacy is in real terms distributed according to wealth and social class.

In the workplace it is most often the case that the lower positions will the ones which are subject to the highest levels of scrutiny. This is despite the fact that malfeasance and

dishonesty at the highest levels of organisations has the potential to cause widespread social damage as the numerous Irish banking scandals have shown. Managerialism and the concurrent values associated with the prevalent discourses of performance management have monitoring and surveillance at their core. Frederick W. Taylor devised his scheme of scientific management to solve the problem of managerial control, 'how can managers ensure the maximum degree of effort for minimum amount of reward?'(Grint 2005, p. 177) Solving this problem involved the division of complex labour processes into the smallest conceivable elements, each of which could be carried out repetitively by one person at a speed far greater than if one person undertook the process in the original fashion of from start to finish. At the core of Taylorism is the surveillance of workers by management; this surveillance takes the form of a constant measuring of performance and productivity and the comparison of these measurements with management defined norms or targets. Contemporary work practices which are facilitated by digital technologies, allow for much higher levels of measurement as every computer keystroke can be recorded, stored, and retrieved to form an evaluative basis for performance management. As well as monitoring performance, workers can have their general behaviour monitored by their employers both inside and outside of the workplace. Work emails and computers are routinely monitored by employers individual times of entry and exit and even the number of trips to the lavatory can be recorded through the use of swipe cards. In 1913 Henry Ford famously had the department of Sociology in his Chicago plant monitor his workers outside of work hours to ensure they were living virtuous lives that deserved the five dollars a day salary they were paid. Ford's sociology department instructed employees in the ways of virtuous living by ensuring that they embrace values such as modesty, sobriety and thrift and reject 'debauched' behaviours such as drinking. Variations of this organisational behaviour have occurred recently where for example workers in a German supermarket were secretly recorded while they were in the break room with the aim of management building a picture of the lifestyles led by their employees (Fuchs 2010, p. 109). The manner in which surveillance practices are embedded in the processes and practices of work will be examined closely in chapter five.

### 3.8 Legal Perspectives

Now that the theoretical approaches to privacy have been explored; it is necessary to perform a brief overview of the legal approaches to defining and regulating privacy. Ireland's privacy laws are a mixture of unenumerated constitutional rights and European Union directives which have been transposed into Irish law. At the level of the European Union article 8 of the European Convention on Human Rights explicitly confers the right to privacy with respect to family life and dwellings. In the constitutional sense there is not an explicitly defined right to privacy, instead other articles of the constitution confer rights which have been interpreted to include a right to privacy. Privacy is thus an unenumerated right as it is inferred from other articles of the constitution in particular article 40 which deals expressly with personal rights. Included in this article is section 5 which deals with the inviolability of the dwelling places of citizens; the focus on the home as a space protected from the prying of the state is further emphasised in article 41 which deals with the family.

This marking out of private space within the family home is consistent with the traditional conceptions of privacy outlined above, that it is a space which much be protected from 'invasion' from outside forces. Judgements of the Supreme Court have also touched upon aspects of privacy such as for example the right to marital privacy which was ruled on in the 1974 McGee vs Attorney General case, in this instance the issue for judgement was the import of contraceptives. The status of the home as inviolable has been criticised from a feminist perspective (Allen 1988) (MacKinnon 1989) as it gave a shield behind which crimes such as domestic violence and abuse could be carried out. Interestingly the rights bestowed by the constitution are subject to the common good and public morality, which by any reckoning are broad and potentially contestable concepts.

With regard to personal data; Irish law uses two data protection acts (1988 and 2003) as the basis for regulation. The data protection model is based on Westin's conception of privacy described above, namely that people 'determine for themselves when, how and to what extent information about them is viewed by others' (Westin 1967, p. 7). Data

protection is concerned principally with rules for the gathering, handling, maintenance, and use of personal information. Data protection law is informed by the 'principles formulated by the OECD and the European Council as early as 1980' (Van Dijk 2006, p.149). These principles include the use limitation principle, the principle of purpose specification, the principle of transparency or openness, and the principle relating to the quality of the data held. (Van Dijk 2006, p.150) In the language of data protection the individual is referred to as a data subject and has a list of rights associated with these principles which include the right to know if details are being held, the right of access, the right to remove or change any details held, and the right to object to personal details being used. The underlying aim is to give data subjects a right to know who has information pertaining to them, how and why they have this information, and to check its veracity.

The rights of data subjects are matched by responsibilities of data controllers; any person or organisation that holds personal information is bound by the data protection acts to keep within the principles of data protection. These principles deal with how the data is obtained, how it is used and how long it is kept for. In order for data controllers to be fair and transparent they must only use the data for the purposes described at the time of collection, and they must ensure that the data subject is aware when their data is being collected. The principles of fair processing are thus similar to the principles of informed consent insofar as the data subject must give permission for their data to be collected and stored, and in order to give this permission they must be furnished with all the relevant details necessary to make an informed decision. A further element of data protection legislation relates to data which theoretically no handler is allowed to process which includes categories on race and ethnicity, sexuality, health, union membership and political views.

While the EU standards on data protection are among the strongest in the world they do come with extensive shortcomings. 'Firstly the act is not about privacy per se. Rather it provides a set of rules for the processing of data' (Working Group on Privacy 2006, p.23). These rules may be increasingly important in the networked world but they are

not and do not claim to legislate for privacy. It is possible for a person to be watched, listened to or placed under surveillance without them receiving any protections from the data protection act. The fact that the basis for these acts were formed in the 1980's means that they are also behind the times technologically speaking. The fast pace of change with respect to technology in general and the internet in particular makes adequate legislation increasingly difficult. A further problem posed is that of the geography of the internet, while data protection legislation is binding inside the EU; the internet is a dispersed network and many sites are located and operated outside of the EU and are thus not subject to its laws. As well as this the data protection regime creates a need for bureaucracy and is expensive to operate, a cost which is borne by businesses. Lastly a problem with data protection is that it assumes that all people are adequately informed to know how to invoke their data protection rights.

### 3.9 Privacy vs. Surveillance

There are a number of scholars who argue against the idea of privacy being the answer to increased surveillance. (Gandy 1993) (Lyon 2001, 2002, 2007) (Stalder 2002). These arguments are based around the idea that contemporary data gathering and mining techniques have reached such a level of prominence and sophistication as to render the notion that some information is private irrelevant. The Panoptic Sort written about by Gandy in 1993 describes the political economy of personal information where all information about a person is valuable as it adds to the overall picture used to create a marketing profile. The aggregations of these data are used to 'sort' people according to inferred consumer behaviour and other elements such as inferred income. The conclusions drawn about the individual throughout this process form the basis of how the individual is treated by certain institutions such as in the context of insurance, inferred behaviour which could be described as risky leads to a higher premium. In this sense the pervasive gathering of data that accompanies contemporary living is seen as feeding the process referred to by Gandy as the Panoptic Sort (1993) and by Lyon as Social Sorting (2002). Much of this information simply constitutes the flows of contemporary living, and while any individual piece of information may seem insignificant and thus not included in the remit of *private* information; when the whole

gamut of these data flows are pieced together they form a supposedly accurate portrayal of the individual. Thus the notion of some data being private and other data being acceptable for gathering is somewhat redundant as potentially all data than can be gathered is usable to ascertain knowledge about the individual.

The given dichotomy of private and public information is also spurious at best (Sheller and Urry 2003, p.122) (Nissenbaum 2010) as there is constant flows between public and private information. Public information such as legislative proposals, voter registrations, election materials, newspaper reports court proceedings and so on are now freely available through electronic networks, yet this availability makes this public data amenable to private use. Financial institutions can use voter registers to compile marketing lists, court judgements can be compiled and used to categorise and assess individuals according to perceived risk. Conversely private information held on electronic networks can be subject to public scrutiny through both legal and illegal means; legal being state mandated surveillance, or targeted marketing practiced by corporations, illegal including such activities as identity theft and hacking.

A further critique of privacy comes from Gilliom (2001) who sees little in the 'rights discourse' of privacy that would be useful to the very people who need protection. Gilliom (2011, p. 500) describes the 'intellectual regime' of privacy which posits it as being at the opposite end of a diametric spectrum from surveillance in a position which polarises the two concepts. This regime according to Gilliom omits core issues such as power, context and conflict. Gilliom in 'Overseers of the Poor' studied welfare applicants and recipients in rural Ohio and their responses to the data matching initiatives which aimed to crack down on welfare fraud. The subjects of Gillioms study were uneducated rural and impoverished women and they did not possess the cultural, financial or legal capital necessary to avail of the right to privacy as enumerated by the discourse of rights. This critique of privacy is in keeping with the point noted above that access to privacy is often distributed along lines of social class and the concomitant aspects of cultural and financial capital.

# Chapter four: Surveillance

## 4.1 Introduction

This chapter will look at sociological and criminological descriptions of surveillance and aim to place it within the broader theoretical context of social and technological change. The first aim is to generate an operational definition of the term which goes beyond the vernacular understanding. Following this; bureaucratic organisation and its use as a means of governance will be looked at with particular reference to Max Weber. Bentham's Panopticon will then be discussed within the context of Michel Foucault and his writings on power, subject formation, the disciplinary society and biopolitics as well as Thomas Mathieson and his complementary theory of the Synopticon. The post-modern theories of the control society will also be briefly looked at in detail with particular reference to surveillant assemblages and the rhizomic structures of surveillance as well as the work of Bogard and the notion of disarticulation of power, control, and identities.

## 4.2 Defining Terms

The word surveillance is etymologically derived from the French word surveiller which means to watch over. Surveillance is defined in the Penguin English Dictionary as 'close watch being kept over somebody, e.g. by a detective' (2002). This definition is typical of the embodied and ocular definition of surveillance; it describes the physical act of an embodied person or group of people being watched by another person or group of people. A further element of note in this definition is the example of whom the watcher would most likely be 'e.g. a detective'. In common parlance surveillance is a value laden term with which there is an implicit association with wrongdoing. A person who is under surveillance is a person of interest to law enforcement, a person who is suspected of committing a crime in the past or future and is therefore a legitimate target to be watched. While this definition no doubt describes relatively common social practices, it is too narrow and only describes the negative aspects. A mother watching her child at play, a lifeguard scanning the shoreline, a doctor monitoring a patient's heart rate or

blood pressure are all further examples of surveillance which infer no element of wrongdoing and instead would describe acts of caring. In this sense surveillance is Janus faced in as far as it can be a process which enables just as easily as it can be used to constrain.

Yet even including these examples in a definition of surveillance still excludes a vast and ever increasing field of surveillance; that of the monitoring of digital traces. Contemporary Irish society is one which is increasingly mediated by digital technologies; for example in December 2011 the Central Statistics Office reported that 78% of all Irish households had access to the internet which was up from 57% in 2007 (CSO 2011, p. 5). The take up of internet enabled smart phones is predicted to increase (Amarach Consulting 2012, p. 9) and the use of social networking is estimated at around 68% of the population (Comscore 2012, Ipsos Mrbi 2012). As well as telecommunications and the internet there are also a number of other processes which are prevalent, for example; loyalty points cards for shops and supermarkets, and credit and debit cards for undertaking financial transactions. The point of note with all of the above- mentioned items is that they all generate data trails which can offer telling clues as to the kind of lives being lived by their users, or to put it in other terms 'data is the perspiration of the information age' (Solove 2004, p.19). This form of monitoring of digital remnants is referred to by Roger Clarke as dataveillance (Clarke 1988). Bearing in mind the extension of meaning of the word surveillance to include actions of caring, and to include the process of dataveillance; a more apt definition would be that from David Lyon. He says surveillance is 'the focused systematic and routine attention to personal details for purposes of influence, management, protection or direction' (Lyon 2007, p. 14). In this definition personal details refers to the persons observable actions just as much as the digital traces left behind and there is also the extension of the reasons for surveillance taking place beyond that of the implicit suspicion definition offered above.

When discussing surveillance the focus is often on state actors and how they use surveillance methods. While this is true, emphasis must be placed on how much private

companies and corporations use surveillance measures as a means of generating business and ensuring operational efficiency. Or as Amatai Etzioni claims it is not ‘big brother’ which should concern us but ‘big bucks’, (Etzioni 1999, p. 139) the use of surveillance by private enterprises as means of managing their customers will be looked at in detail in chapter seven.

Fuchs (2011, p. 111) has written of how surveillance is typically defined in academic circles either as negative; and so concerned with domination and the exercise of power, or as neutral. The neutral side of surveillance is typified by the positive examples above which are widely based around surveillance as a means of enabling or caring. A further element of neutral surveillance is the assertion that surveillance is built into contemporary societies due to the workings of complex bureaucracies and the nature of life in information societies. Fuchs (2011, p. 123) rejects the separation between neutral and negative surveillance and instead divides his definition between economic surveillance and state surveillance. Economic surveillance includes any forms of consumer surveillance and any form of workplace monitoring or managerialism. State surveillance includes law enforcement, population enumeration, and any other activities of any arms of the state which operate to ensure its security and efficient operation. Fuchs however doesn’t seem to mention any examples which fall between the two terms such as the enforcement of taxation, which involves mass monitoring and surveillance and falls in the remit of both economic and state.

### 4.3 Weber and the Bureaucratic Method

To properly describe surveillance it is also necessary to give a brief historical summation of its roots in social and sociological thought. Max Weber wrote extensively and authoritatively on the nature of bureaucratic organisation and its role in the formation of nation states and other forms of control over the complex organisations which are the bedrock of modern societies. ‘It is obvious that technically the large modern state is absolutely dependent upon a bureaucratic basis. The larger the state, and the more it is a great power, the more unconditionally is this the case (Weber translated by Roth and Wittich 1968, p. 971).Bureaucracies by definition are information hungry organisations

that operate through the routine gathering and utilisation of information. The types of organisations written about by Weber predated computers and digitisation; yet they still adhere to the same core principles that govern contemporary institutions. These principles are based around the need for institutions to be 'logical, rational and efficient' (Miller 2011, p.121).

The first element of a bureaucracy is that of delimited jurisdictional areas 'which are generally ordered by rules, that is by laws or administrative regulations' (Weber 1968, p. 956). This meant that the practice of rule is conducted in a hierarchical and procedural manner which contrasts sharply with the earlier systems of patrimonialism and serfdom which were often based on the whims and fancies of a ruler. Patrimonialism also allowed for decision making to be tempered by bribery, dishonesty, favoritism or emotion. The bureaucratic form of organization vests power in an office holder who has strict rules and regulations which govern how it can be exercised. Thus it is more the office holder than the individual who wields this regulated and delimited power.

> 'Individual performances are allocated to functionaries who have specialized training and who by constant practice increase their expertise. "Objective" discharge of business primarily means a discharge of business according to calculable rules and "without regard for persons"' (Weber 1968, p. 975).

The objectivity of bureaucratic organization is what Weber claims makes it calculable and therefore predictable and rational; decisions are made according to the rules and thus there is no room for personal intervention or favoritism.

The principles of hierarchy and rank are also important to bureaucracies; each office has subordinate and super-ordinate offices which allows for an appeal of any decisions made by one office to a higher power. At the time of Weber writing, the running of bureaucratic offices did not differ much according to whether they were public, private or religious enterprises. They all operated on paper- based record keeping or files which

meant that all decisions and actions of the bureaucracy were to some degree transparent, rule based and historically searchable thus inculcating a degree of institutional memory.

### 4.4 Bentham, Foucault and The Panopticon

While the core metaphor used in common parlance when talking about surveillance is Orwell's 'Big Brother'; the ubiquitous metaphor in surveillance studies is the Panopticon. This was a model for a prison which was originally written about by Utilitarian philosopher and social reformer Jeremy Bentham in the late eighteenth Century. It was in fact Benthams brother Samuel who had the original idea; but it was Jeremy who developed it and wrote about its potential for social reform. Bentham envisaged his design as being not just a prison but an 'inspection house' which was

> 'applicable to any sort of establishment, in which persons of any description are to be kept under inspection; and in particular to penitentiary houses, prisons, houses of industry work houses, poor houses, lazerettos, manufactories, hospitals, mad houses and schools'(Bentham 1995, p. 29).

The idea for the Panopticon was elaborated in a series of letters written by Bentham in 1787, and to him it was not just an efficient means of operating the above named instutions but was also a viable plan for widespread social and disciplinary reform.

> 'Morals reformed- health preserved- industry invigorated instruction diffused- public burthens lightened- Economy seated, as it were upon a rock-the Gordian knot of the Poor laws are not cut, but untied-all by a simple idea in architecture' (Bentham 1995, p. 30)

The defining aspect of the Panopticon is that of visibility; the circular building is designed with a central observation tower which every cell faces. The cells are back lit which make them and their occupants constantly visible to the inhabitant of the inspection tower. The key however is that the inhabitant of the inspection tower is invisible to those in the cells and thus power is tied in with visibility; with the powerful

being invisible and the subjects of power being constantly visible. The gaze from the inspection tower is unverifiable and so the inmates must assume that they are under constant observation and act and behave according to the prescribed norms of the institution. Bentham saw this not as being just a means of controlling inmates or maintaining order inside institutions; but as being a 'new mode of obtaining power over mind, in a quantity hitherto without example' (Bentham 1995, p. 30). This 'power over mind' would allow for proper and effective rehabilitation of inmates and would act as a mode of re-socialisation where errant ways of being could be corrected in a fashion similar to orthopaedic correction. Whereas orthopaedic methods corrected physical deficiencies; the panoptic method could correct social or behavioural deficiencies through the constant surveillance of inmates with the aim of keeping them close to prescribed norms of behaviour or normalising judgements to use Foucault's terminology.

> 'It is obvious that, in all these instances, the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose X of the establishment have been attained.' (Bentham 1995, p. 32)

The utility of the panopticon design is that it takes into account the fact that it is impossible to constantly inspect all inmates and in practice it does not try to do so. Instead the aim of the design is to make the inmates believe that they are under constant inspection and compel them to behave accordingly. The Panopticon is thus a machinery of power, in practice it is irrelevant whether or not the observation tower is occupied, what matters is that the inmates *believe* that it is occupied and behave accordingly.

> 'Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should render its actual exercise unnecessary…… in short, that the inmates should be caught up in

> a power situation of which they are themselves the bearers' (Foucault 1977, p. 201).

While there was no prison built to his specifications in his lifetime, the east wing of Kilmainham prison in Dublin which was built in 1863 was built with a quasi panoptical design where all three floors are visible from a central point and 'all prisoners were constantly watched through special spy holes built into the door of each cell' (O'Sullivan 2007, p. 16). This Victorian design however was for separation and surveillance of inmates for the purpose of giving them time to reflect on their 'sins'; other prisons which have been claimed to be Panoptical such as Pentonville in London are similarly designed. These prisons are not in the strictest sense built to the specifications of the Panopticon; while there is a centralised point from where all cells can be seen, the cells have closed doors and so the Benthamite conception of complete visibility is not apparent. The closest a prison has come to being truly Panoptic in structure was the Presidio Modelo or model prison built in Cuba the 1920's. This prison consists of four panoptical structures and a fifth building which served as a residence for the guards and other staff but was closed down in the 1960's after riots and hunger strikes caused by severe overcrowding. The Benthamite ideals of separation and surveillance of inmates as a philosophical project of self reconstruction often fell foul to harsh realities of economics. In Kilmainham as in the Presidio Modelo overcrowding meant that the cells which were designed for an individual were frequently occupied by groups of people. Thus the underlying philosophy of the 'silent, separate, system of observation' (O'Sullivan 2007, p. 16) was effectively stymied by the needs and practices of the institution.

While Bentham had some interesting ideas with regard to penal policy and the rehabilitation of prisoners, it was Michel Foucault who used these ideas to underpin his schematisation of the Disciplinary Society (1977). Foucault saw the writings of Bentham as being emblematic of a new form of discipline, a new mode of exercising power which was productive rather than destructive. Using what Foucault terms discourses; this new form of power created obedient subjects rather than simply obliterating the disobedient.

Whereas older forms of discipline physically and brutally punished deviations from the rule in the form of public spectacles of violence and power; the aim of disciplinary power is to inculcate and to teach, so that the norms and rules become internalised thus creating useful, productive and law abiding citizens. 'The right to punish has been shifted from the vengeance of the sovereign to the defence of society' (Foucault 1977, p. 90). Discourses are 'sets of deep principles incorporating specific grids of meaning which underpin, generate and establish relations between all that can be seen, thought and said' (Schilling 1993, p. 66).

Discourses are concerned with the manner in which language and power organises fields of knowledge which can in turn be used to create the subjects they are supposed to be describing (Foucault 1972 pp. 24-25). While it was originally the norms and rules of the given institution such as the school the prison or the hospital which were to be internalised; Foucault sees these techniques of 'soul training' as being replicable in wider social processes and being central to subject formation and in particular the creation of 'docile bodies' which are amenable to instruction. 'A body is docile that may be subjected, used, transformed and improved' (Foucault 1977, p. 136). Central to Foucault's conception of Panopticism is the gaze of power, which is hierarchically organised so that those in positions of power monitor their subordinates. This hierarchical observation involves the viewing of the many by the few which is in contrast to Mathieson's (1997) conception of the viewer society where the few watch the many. A further element of panopticism is the compulsion for classification; in such institutions all inmates are classified for the purpose of measuring compatibility with prescribed norms. 'New prisons developed a form of spatial and temporal control via hierarchies of surveillance and classification and sought to instil discipline over a prisoners body through disciplining the mind' (Coleman and McCahill 2011, p. 16).

It was when these techniques spread outwards beyond the walls of the prison the hospital or any other carceral institutions that the disciplinary society was born. Panopticism and surveillance were not just used to counter or correct criminals or the insane but were also used in a more generalised sense to ensure collective adherence to

norms. Thus the normalising judgements passed through the gaze of authority and watched everyone, not just in the institutions but in society at large, until the gaze was ubiquitous and constant and forms of self policing and self inspection were inculcated in a 'docile' citizenry who accepted predominant social norms.

The subjects created through the exercise of power are subject to power/knowledge; as mentioned above, the exercise of power can be productive in so far as subjectivities are created and categorisation occurs. In the process of categorisation there is a considerable exercise of power in the form of decisions of inclusion or exclusion, membership or otherwise within each category. While the panopticon and the attendant carceral techniques of soul training acted on the individualised body; Foucault's writings on governmentality and in particular bio-politics relate to the mass of individuals or the body politic as an object of enquiry.

> 'Biopolitical government refers more specifically to a strategical rationality for the management of population, understood as a vital resource. Through the deployment of various normalizing technologies of power, biopolitical government seeks to organize population so as to maximize its value as a resource' (Rayner 2001, p. 148).

With disciplinary society came a switch in focus from the body and the flesh to the mind and it's actions and intentions, biopolitical governance involved a further switch in the focus of discourse from the individual to the population. The focus on the generalised body politic was based around the marshalling of the population with the aim of maximising its power as a productive resource. This meant that public health, demographics and other discourses of population came to prominence. In terms of surveillance; the institutions of the state became actors in the collection, collation and reporting of information relating to the population (Foucault 1978-79). The census aimed to know exactly how many people lived in the territory, how many of them were of working age, how many were eligible for taxation, it also aimed to know through birth and death rates if the population was replenishing itself. The census as a technique

of governance and exercise of power is ancient; at least as old as William the First and his famous census of 1086 which came to be known as the Doomsday Book. If Biblical sources are considered, then the census can be seen to be even older as it was for the purpose of enumeration that Mary and Joseph left Galilee to go to Bethlehem.
As well as the census other pre-existing institutions were able to act as knowledge brokers for the state, for example schools could give a barometer of child nutrition and general health. Lyon describes how knowledge of individuals and populations has continued to be relevant outside of disciplinary and punitive measures of the state. Using the context of legibility and eligibility Lyon describes how in order for citizens to claim the rights and entitlements afforded by their governments –eligibility- it is necessary for the same citizens to be transparent and identifiable –legible-(Lyon 2009, p. 46). Where people are legible and therefore identifiable and connected to their records, it makes it possible for the administration of rights and entitlements by state actors and institutions.

### 4.5 Sousveillance and the Synopticon

As we have seen above the word surveillance is derived from the French word surveiller meaning to watch over and watching over someone often denotes a relationship of authority. There is however the obverse of surveillance; where watching is done from below, where the person or people subject to authority watch the figure of authority. This is called sousveillance (Mann 2004, p. 620) which translated from French means literally to watch from below. Sousveillance as a practice has its roots in the cyborg experiments of people like Mann (2003) who connected cameras and other wearable computing and media capturing devices to their bodies and set about recording their lives, other projects such as the Life Logging project (Bell and Gemmell 2010), or the quantified self take on similar tasks while utilising similar methods. While these experiments could arguably be seen to be on the cutting edge of human computer interface (HCI) and cyborg research, the broader questions regarding the fusion of humans and machines will not to be examined here. The sousveillance aspect of these projects raises interesting questions regarding surveillance actors and power relations. In the case of Mann (2003) his experiment involved the wearing of eyeglasses which had

small cameras attached to them which would record all that he had seen. The cameras while being small were noticeable and led him to situations of conflict especially in places where surveillance was at its most intense.

> 'the author, through simply a personal desire to live in a computer mediated world, encountered hostilities from paranoid security guards, seemingly afraid of being held accountable. It seemed that the very people who pointed cameras at citizens were the ones who were most afraid of new inventions and technologies of citizen cameras.' (Mann 2003 p625)

It is the process of holding others accountable -especially those in positions of power- that characterises sousveillance. The most famous sousveillance footage is that which depicts the Los Angeles police assault on Rodney King in 1991 which sparked widespread rioting. Mann conducted his initial experiments over a period of twenty years which encompassed the 1980's and 1990's, since then mobile phone technology has advanced and internet enabled camera phones are approaching ubiquity. The increasing popularity of camera phones and the ease of dissemination of video footage through the internet mean that there is now a maelstrom of different viewpoints from which any event is likely to be recorded. Komarova and McKnight (2012) examined the use of photography during contentious parades in Belfast in 2011 and noted 'the dense mesh of digital gazes and glances' (2012, p. 28) as every participant and observer on the scene filmed the event through either cameras or mobile telephones. This meant that there was a panoply of digital viewpoints from which the parade could be watched as participants filmed protestors, protesters filmed participants, the Police filmed both and the researchers filmed the scene. If any major sporting, political, social or cultural event at which there is a large audience is searched for on Youtube; it will be seen that this 'dense mesh of digital gazes' is evident. As cameras have become ubiquitous such events have commonly become subject to filming by observers which means that events are visible in a broad scope and from many angles which 'heralds the emergence of competing narratives' (Komorova and McKnight 2012 p29).

As well as this many events which would previously be unseen are now recorded and disseminated globally. If we consider the case of Mary Bale –or the 'cat bin lady' as she is infamously known- we can see this in action. In this case a woman who puts a cat into a bin is caught in the act as the cat's owner had installed a CCTV camera on his house. The facts of multiple, camera mediated viewpoints and the ease of dissemination through the internet in general and social media in particular mean that acts such as this can be filmed and displayed to the world with ease. This has led to what Fraser has described as 'a networked, horizontal, multi-mirrored Panopticon in which everyone can spy on everyone else' (2011, p. 2). This ability for 'lateral surveillance' (Andrejevic 2005) means that surveillance is to some degree de-centred and the capability to monitor and record is spread throughout the population. The gaze of surveillance therefore is not just 'top down', it can also go from the bottom up; this can be seen in organisations such as Copwatch who actively monitor police activity and where possible record police misadventures. The most famous and recent instances of sousveillance which have impacted whole societies are evident in the Arab Spring of 2010 where official narratives were supplanted by protesters recording and distributing footage of state violence.

In the Irish context the methods of the policing of the 'Shell to Sea' protests in Rossport Co. Mayo have also generated controversy through the unwitting use of sousveillant methods. The most famous instance being that of the so called 'rape tape' where a camera confiscated from a protestor was left running in a Garda patrol car. While the camera lens was covered, the camera still recorded sound and the conversation between the Gardai made reference to raping the owner of the camera. The recording was made accidentally and without the Gardai in question realising, and when the camera was returned to its owner the offending footage was posted to the internet garnering much media attention and debate (Siggins 05/04/2011 Irish Times).

While sousveillance can result in the holding to account of the powerful such as in the cases mentioned above; it is more often than not the case that holders of institutional power remain in control of such situations. It is these people who more often than not

control what Goffman describes as the definition of the situation through having the power and the know how to contextualise any footage and to seize the initiative in shaping the narrative of events through the use of public relations personnel. While the ability to disseminate has been made easier through the internet, it has also made it more difficult to gain attention. Even if a clip can be posted on Youtube; if the news agencies ignore it then it does not become a credible story. So while sousveillance can and has been used to effectively hold powerful people or authority figures to account it is still the case that due to both institutional and economic power differentials sousveillance is predominantly ineffective as a counterpoint to panoptic power. 'While in principle everyone can indeed watch everyone else, in mediated ways- screening the results- some forms of watching carry more weight than others' (Lyon 2006 p39). Instead the spread of sousveillance has created the situation where potentially any activity or place is covered by camera and almost any footage can go 'viral' which has lead to what Fraser (2011) has termed the 'unblinking panopticon' This means that conceivably almost any action in public and many in private spaces can end up being filmed and disseminated for a global audience.

While the primacy of Foucualt's panoptic scheme has been noted above it is also important to mention his omissions. Discipline and Punish was written in the 1970's and was intended by Foucault to be a historical look at general forms of discipline and surveillance with the aim of seeing how they inform the present. But still Foucault's work does not include any reference to more contemporary concerns such as the mass media, consumerism and the role of technology particularly computing. At the time of the writing of Discipline and Punish the first two would have been prevalent and the third would have at least been known to Foucault. Despite these omissions other writers have taken up these concerns most notably Mathieson and his synopticon or viewer society thesis (1997). There are two core features of panopticism, firstly there is the imbalance of power as is evident in it's description being the few watching the many; and secondly panopticism is concerned not with just 'viewing' but instead is based on the ability of the viewer to influence or coerce the viewed. In Foucault's telling, the disciplinary society was preceded by the age of punishment as spectacle; where

punishment was directed at the body and took the form of public displays of violence and retribution such as public executions, hangings, or floggings. Yet a further element in the spectacle of power was the lavish displays of wealth which were evident in royal parades, military displays and even in the design of palaces and other state buildings. In the movement towards disciplinary society the former types of display were first moved from the public eye and to the inside of the prison and ultimately were discontinued as rehabilitation and reformation came to replace annihilation as a form of punishment. Key to the viewer society thesis is the latter type of display; which instead of being moved out of sight was moved onto the newspaper pages and television screens.

As mentioned above the panopticon involves the gaze of power where the few (ie the powerful) watch the many (ie the less powerful/powerless). Thomas Mathieson noted how in concert with panoptic methods and practices there was what he termed the synopticon which he describes as 'a unique and enormously extensive system enabling *the many to see and contemplate the few* so that the tendency for the few to see and supervise the many is contextualised by a highly significant counterpart'(Mathieson 1997 p219 italics in original).

It is through the contemplation of the many that the core processes of synopticism operate; through the mass media it is possible to see the powerful, wealthy and successful few whose stories and images are displayed as examples to be followed by the many. It is thus at the level of culture that success stories are disseminated, stars of entertainment, sport or any other form of public life are players in the newer form of display. The examples set by them whether through following their success or mimicking their patterns of consumption; create another set of norms which operate in tandem with those set through panoptic methods. The core difference of course being that synoptic power operates through its visibility. Whereas panoptic power is that which is hidden and unknowable, synopticism operates through displays which are offered as examples to be followed or avoided depending on the context (Mathieson 1997, p. 228) (Baumann 1998, p. 52). Where panopticism operates through coercion, -or at least the threat of coercion- synopticism operates through seduction or inducement towards

particular culturally desirable behaviours. In the panoptic sense the few watch the many in order to ensure compliance with and to root out deviations from the norm. In the synoptic sense the many watch the few in order to be acculturated and be taught what the norms are. If the panopticon relates to the invisible watching of power, then essentially the synopticon relates to the broadcasting of power (Mathieson 1997, p. 225). Through the mass media synoptic messages are displayed which show the viewers how they are expected to live, the norms they are expected to uphold, the goals they should aim for and the legitimate means available to them to achieve these goals.

It is not just through emulation that synoptic power operates; there are many contemporary examples which show modes of behaviour to be avoided, for example television shows such as "worlds dumbest criminals" use CCTV footage from bungled robberies to ridicule the perpetrators (Doyle 2006, p. 199). Chat shows which run on heavy rotation to an international audience routinely feature human interest stories of people who have suffered due to their involvement in illicit drug use, alcohol abuse or promiscuous sexual behaviour. These stories bear synoptically on their viewers, acting as warnings, as paths which must not be followed and must be avoided at all costs if the viewer wishes to avoid the tribulations and degradations of those featured. In some ways these tales offer a solid example of the symbiotic relationship between panoptic and synoptic. Stories of criminality, of murders or organised crime for example are more often than not gathered through the exercise of panoptic power such as through law enforcement use of covert surveillance, through CCTV or through testimonies of prisoners. These stories which are gathered panoptically are diffused and disseminated synoptically through the mass media especially through tabloid newspapers and television. When these stories are retold synoptically 'the material is purged of everything but the purely criminal- what was originally a small segment of a human being becomes the whole human being- whereupon the material is hurled back into the open society as stereotypes' (Mathieson 1997, p. 231).

The panoptic/synoptic symbiosis continues when these one dimensional criminal stereotypes are used to create 'moral panics' (Cohen 1972, p. 1) which in turn lead to

further calls for more panoptic measures such as CCTV cameras, more police powers stricter laws or more prisons in a continuing and self reinforcing feedback loop.

While the synopticon is closely bound to the operation of the mass media this does not mean that it is new or that synoptic methods were not in operation beforehand. The example given by Mathieson is that of the Catholic church which through the sacrament of confession allowed the few (ie the clergy) to know the many while at the same time through services, sermons and so on the same clergy also gave examples or models of behaviour to be seen and contemplated by the many (Mathieson 1997, p. 222). Mathieson even includes the Catholic architecture as being part of its synoptic power due to the positioning of imposing and awe inspiring cathedrals and churches in the centre of towns (Mathieson 1997, p. 223). This duality of being simultaneously panoptic and synoptic is also evident in digital television, which operates synoptically through the process described above, and operates panoptically as digital set top boxes can record channel surfing habits, movies watched, advertisements seen and so on, mostly without the knowledge of the viewers.

The interplay inherent between surveillance/sousveillance, panopticon/synopticon creates the situation where there are a plethora of different modes and means of surveillance, and a multitude of vantage points. No single model encompasses the full range of viewpoints and power relations and it is the case that the contemporary surveillance landscape is best described using a mixture of the above concepts. The interplay of which has led to what Lyon (2003, p. 21, 2006, p. 35) has described as scopophilia. This term; which is borrowed from film studies and psychoanalysis means literally a love of looking and Lyon uses it to describe the overarching contemporary cultural norms that are engendered by the prevalence of both television and the cinema. ‘it is not too much of a stretch to suggest that part of the enthusiasm for adopting new surveillance technologies … relates to the fact that in the global north…. the *voyeur gaze* is a commonplace aspect of contemporary culture’ (Lyon 2006, p. 49).

Taking into account a wide spectrum of popular culture such as reality television, repackaged CCTV clip shows, movies, novels and the mass media in general; Lyon claims that watching or 'viewing' has become a central tenet of general culture. This normalisation of viewing has had a twofold effect, firstly people want to see and secondly they want to be seen. Although not mentioned directly by Lyon this acculturation to the seeing/being seen dyad could be offered as an explanation for the ever growing popularity of social networking. Scopophilia in these terms contributes to the prevalent culture of display which is evident in social networking, reality television and celebrity culture. This culture of display will be examined in detail in the conclusion chapter.

### 4.6 Surveillant Assemblages

A further misconception regarding surveillance is that of who conducts it; typically as we have seen above it is thought that surveillance is conducted or supervised by a single entity. This mode of thinking has its roots in the earliest theories of surveillance from the Panopticon of Foucault to Orwell's sinister figure of Big Brother. This schematisation however is partially incorrect; in fact the picture is more complicated with a much larger and amorphous collection of groups which tend towards 'assemblages' (Haggerty and Ericson 2000) that are capable of surveillance. These assemblages are 'a coming together of disparate elements to create a loosely associated surveillance entity' (Lyon 2007, p. 95) 'a multiplicity of heterogeneous objects whose unity comes solely from the fact that these items function together, that they "work" together as a functional entity' (Patton 1994, p. 158 Quoted in Haggerty and Ericson 2000, p. 106). Thus seemingly discrete systems of surveillance which capture 'information flows' (Solove 2004, p. 3) are in fact rarely discrete as there is a tendency towards convergence in these systems as they are joined up or concatenated to form 'surveillant assemblages' (Haggerty and Ericson 2000, p. 106). An important point of note is that of terminology; while in Haggerty and Ericson reference is made to "the" surveillant assemblage, it should not be seen as a unitary or monolithic entity. Instead the assemblage should be seen as an unstable collection of interlinked potentialities. These assemblages are loosely affiliated entities with operational imperatives determining the scope and circumstance of the links

which are maintained across institutional and state borders. Central to the theory of assemblages is the manner in which they aim to interrupt the flows of life; in striating or creating breaks in these flows the assemblages are capable of capturing data and creating bounded spaces of comparison. Delueze and Guattari thus differentiate between the concepts of power and force in their explanation of assemblages; force is the elementary strength found in the flows, and power is that which is derived from systematically harnessing them (Haggerty and Ericson 2000, p. 106). While assemblages are multiple and amorphous, there has been and continues to be instances where state actors have reigned in and centralised or co-opted them for their own use. The most famous examples can be found in the aftermath of both the September 2001 and July 2007 terrorist attacks in New York and London. In both instances the rhizomatic shoots of information regarding those responsible such as their travel data, their financial data and their phone records were effectively gathered and centralised by the security services. So in this sense there was a rhizomatic levelling; when necessary the state and its centralised apparatuses could impose themselves and gather in the dispersed elements of data left behind. 'The surveillance *state* shows itself to be stronger than ever, even though it now uses the dispersed systems and devices of the surveillance *society*' (Lyon 2003, p. 37 italics in original). Even if surveillance is characterised in terms of dispersed rhizomatic elements which bear little relation to each other; it is possible for powerful actors like the state to rein them in to a centralised grouping.

### 4.7 Data Doubles

In writing of the disciplinary potential of the panoptic methods of 'soul training' Michel Foucault placed the corporeal embodied person at the centre of discipline (1977, p. 135). It was the embodied self that was incarcerated and it was at the level of the self that discipline was internalised through the constant yet latent and unverifiable gaze of authority. Contemporary surveillance, particularly through the assemblages is less concerned with the embodied person and is more concerned with the traces it leaves behind. The body 'is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a

decorporealized body, a ‘data double’ of pure virtuality. (Haggerty and Ericson, 2000 p. 611)

Haggerty and Ericson claim that data doubles move beyond the realm of representation or simulation because they are ‘productive of a new type of individual, one comprised of pure information’ (Haggerty and Ericson 2000, p. 614). This claim ties in with that of Mark Poster (1995) who claims that databases can be seen in terms of discourses in so far as institutionally they play a part in the shaping of subjects. Data doubles are formed in the process of breaking down and reconstituting subjects, or ‘disarticulating’ them to use Bogards term (Bogard 2006, p. 63). Institutions use these reconstituted subjects as the basis of decision making. Thus data doubles can be seen as acting on embodied subjects, allowing or refusing, enabling or constraining. This process could be linked to Baudrillard’s hyper reality and the description of the ‘precession of simulacra’ (1983, p. 2) where the map creates the territory instead of vice-versa; in this instance the map is the data double and the territory is the subject: ‘it is no longer a question of imitation, nor of reduplication, nor even of parody. It is rather a question of substituting signs of the real for the real itself’ (Baudrillard 1983, p. 4).

The use of data doubles in terms of their constituting the embodied subject is problematic; the image of the person which is recreated through the digital filters will be distorted and not fully representative. As mentioned previously data collected will only describe particular aspects of the person and form what Solove terms the mosaic. A useful metaphor is that of the hall of mirrors (Johnson and Regan 2011, p. 1) which distorts and exaggerates particular aspects to the detriment of others, while it is a reflection of the subject, it is also inaccurate and distorted. In relation to the field of consumerism Lace has described this using the metaphor of the ‘Glass Consumer’ (2005, p 7) not just because the fact of the personal information economy makes us all more transparent and visible, but also because we take on ‘the properties and capacities of glass- fragility, transparency, the ability to distort the gaze of the viewer’ (Lace 2005, p. 7). In becoming glass consumers it not just the case that more of our lives are visible,

but also we are distorted and misrepresented according to the narrow view taken of us by the data trails we leave behind.

### 4.8 Disarticulation

The movement from disciplinary societies (Foucault 1977) to societies of control (Bogard 1996, 2006) has been and continues to be facilitated by technologies. As we have seen above disciplinary societies relied on technologies of confinement which by their nature were spatially bounded. Institutions such as prisons, schools, and army barracks, enforced discipline through the processes described above of hierarchical observation, normalising judgement and the examination. The exercise of power was thus bounded in both temporal and spatial terms. According to proponents of the control society thesis it is the technologically enabled undoing of these bonds to time and space that is central to the operation of power. Bogard (2006, p. 59) describes the process in terms of the 'disarticulation' of power; where the limitations of geography and time no longer impede its operation. Because these limitations no longer apply, power according to Bogard operates continuously and without prejudice and this has noticeable and interlocking effects on subjectivity, identity, spatial differentiation and the operation of institutions. 'Control is now an inclusive continuous and virtual function, traversing every level and sequence of events, simultaneously molecular and planetary, no longer limited by walls or schedules (Bogard 2006, p. 59).

Disciplinary institutions operated through close monitoring which sought out deviations from the norm which when found were punished forcefully and quickly. These punishments were/are efficient reactions to transgressions. In the control society however it is not merely efficiency that is sought but also what Bogard terms 'preficiency' (Bogard 2006, p. 60). Thus control –or hypercontrol as he puts it- is maintained proactively as opposed to reactively by using computational models and algorithms to work out *in advance* all conceivable potentialities and outcomes and take action accordingly. Bogard sees military evidence of this in the Bush doctrine of pre-emptive strikes and while unmentioned specifically by Bogard the 'pre-crime' unit in Philip K. Dick's Minority Report bears a close resemblance. Preficiency can also be

seen in the Cromatica system used in the London Underground to prevent suicides, Cromatica is an algorithmic CCTV system that is programmed to spot behaviour 'out of the ordinary'. If a person stands on the platform in a tube station for a long time without getting on a train then the system will bring this to the attention of an operator. The reason for this is that 'those contemplating suicide tend to wait on a platform, missing trains before taking their final tragic steps' (Lyon 2001, p. 60). If the system recognises this action then it can prevent it by flagging it for human intervention thus prevention the incident from occurring. The Cromatica example dates from 2001, while it is still in use there are a number of other preficient systems which aim to prevent incidences from happening before they occur. The most famous is the 'predictive policing' program which is in use in Los Angeles California. This system maps incidences times and the type of crimes committed and looks to discover patterns, the use of analytics allegedly has uncovered 'hot spots' and statistical mapping informs the Police when and where they need to be to prevent crime (Morozov 2013, p. 182) (Rowe 2008, p. 213).

The control society as we have seen is one where power and control can operate irrespective of location in space or time. In a number of interconnected ways this has influenced the manner in which spaces are delineated and encoded. A simple example of this can be seen in the figure of the 'telecommuter'. (Castells 2001, p. 231) Through the use of ICT's many workers can operate efficiently outside of their delineated workplace. This means that workers are always available to others be they travelling, at home, or even on holiday and this in turn makes spaces 'hybridized' (Sheller and Urry 2003, p. 109) and capable of 'infinite modulations' (Bogard 2006, p. 62). Lyon (2007, p. 107) describes control societies as those 'in which old lines become blurred-lines that once distinguished police work from private security, or law enforcement from consumer management'. Another example in the Criminological context would be the use of electronic tagging as a replacement for custodial sentencing in criminal matters. The home in this instance becomes hybridised and modulated as a space that is simultaneously a prison, dwelling and potentially even workplace.

## 4.9 Conclusion

The aim of this chapter was to elucidate the term surveillance; it began by outlining the vernacular usage which is broadly concerned with the monitoring of a person or group suspected of wrongdoing. This understanding was shown to be lacking as it focused only on surveillance in terms of negative supervision; for example the watching carried out by police on a person or group implicated in illegal activity. By stretching out the definition to include acts of caring or other forms of positive supervision, a more rounded definition of the term was achieved. Following this was an examination of the historical and theoretical aspects of surveillance including Weber's writings on bureaucracy and the Panopticon as described by Bentham and Foucault. These viewpoints demonstrated how surveillance is a central aspect to the organisation of complex institutions. In the case of the Panopticon the role of surveillance as a means of facilitating the internalisation of social norms to create self disciplining subjects was examined. In these cases however it was only the downward direction of the surveillant gaze –ie powerful to powerless- that was evident. By examining sousveillance which is the watching of the powerful by those below them, and the synopticon as described by Mathieson; surveillance was redefined as a multi-directional gaze that works from the bottom up as well as top down.

In speaking of the gaze of surveillance; this chapter has contended that it is not just acts of physical watching that constitute surveillance. Surveillance is also most commonly tied in with the monitoring of records and digital traces left behind. The chapter concluded with a description of the 'data double' (Haggerty and Ericson 2006, p. 611) and the manner in which it misrepresents and distorts the image of the embodied person.

# Chapter 5

## Surveillance and the Workplace

'The process of work is at the core of social structure' (Castells 2010, p. 216),

### 5.1 Introduction

This section will examine the processes of work with the aim of exploring the role of surveillance in its patterning and organisation. According to Lyon 'working life offers some self-evident starting points for surveillance studies' (2007, p. 33) as many of the forms of supervision originated in the workplace. 'Workplace surveillance can take social and technological forms' (Ball 2010, p. 87) and as such it is necessary to avoid placing undue emphasis on technology. The chapter will begin with a brief outline of the interview process and how it dealt with questions relating to the workplace. The contemporary forms of work in the information society will be examined with particular reference to the new managerialist imperative to 'measure everything that moves' (Marx 1999) that is facilitated by information technologies and the audit trail. Contemporary scholarship on workplace surveillance will also be examined particularly Ball (2010) and used to interpret the information gathered during interviews.

With respect to workplace surveillance the findings to be presented are that the workplace constitutes an ever shifting domain of social relations; as such norms, expectations and roles within it are subject to constant change. Workplace surveillance is increasing due to advances in technology; the thoughts of the researcher at the outset were that the ever increasing levels of monitoring would be resented by workers. This was seen to be the case in a minority of instances; and in a finding which is emblematic of the omni-directional nature of contemporary surveillance mentioned above it was seen that surveillance was used by workers to their own advantage. Record keeping, auditing and any other systems of surveillance used to monitor employee productivity were also used by employees to hold management to terms and conditions of employment. A further finding related to the clear lines of distinction between personal

and professional life, with many participants rejecting outright any practices which mixed the two.

## 5.2 The Workplace

The definition of what constitutes a workplace is one which will always be open to interpretation. If we consider only paid employment then we rule out a considerable number of voluntary, caring, and domestic activities, even paid work would include domestic work such as child minding which is done at home. For the purposes of the present discussion it is paid work that is done outside of the home which will be the focus. The reasons for this are two fold; firstly all participants bar one were employed in such circumstances, and secondly work which happens in a non-domestic workspace is more likely to be subject to managerial oversight making it more relevant for the aims of the study. In the interviews conducted there were a number of questions which related to work; to begin with, respondents were asked what they do for a living, and this was followed by the question how do you feel about being watched at work. This opened up the conversation towards forms of workplace supervision such as CCTV or managerial oversight. The conversation was then steered towards productivity management in the shape of targets or other forms of performance metrics, and then finally towards the subject of testing for drug or alcohol use as well as personality or psychometric tests. In the instances where a person was unemployed or a student, questions were asked which related to past experiences of employment. In later interviews respondents were questioned not just about their present or most recent employment; but about their employment history, this opened up the scope of the interviews and generated far more usable information. Of the fifteen people interviewed; two were unemployed at the time of the interview and another had recently started working after a period of unemployment. As well as questioning these respondents on their past employment, questions were asked which related to their dealings with the Department of Social Welfare. The purpose of this was to attempt to get a bottom up view of recent anti-fraud and labour activation initiatives which have been in force since 2010 in response to the perceived need to ‘manage’ welfare recipients with the stated aim being to lower state spending on social welfare.

## 5.3 Contemporary Forms of Workplace Surveillance

Workplace surveillance is most certainly nothing new; it has been historically synonymous with the emergence of the discipline of management via the practices of Taylorism and Fordism. What is new however is its socially and technically facilitated intensity and omniscience (Wood 1998, p. 136) (Marx 1999) (Lyon 2007, p. 35). Contemporary workplace surveillance takes the form of either the screening of potential employees, or the monitoring or management of employees on the job. In the context of the former there exists an information economy; where multi billion dollar global organisations or 'omnibus information providers'(Nissenbaum 2009, p. 45) such as Experian, Choicepoint or Acxiom which are used to conduct background checks on potential employees. Other elements of the employee screening process include various medical and psychological tests which can vary from a general health check to a drug test to the increasingly popular range of psychometric and personality tests.

## 5.4 Pre-Employment Screening

As mentioned above the recruitment phase is one which is imbued with background checks. When making a decision on whether or not to hire a person, most organisations will utilise a blend of processes including taking in c.v's, conducting interviews and undertaking various personality and aptitude tests. In the case of c.v's and interviews, applicants give a subjective narrative account of themselves and their capabilities; thus among the earliest phases of the process is third party verification of all claims made at this stage. If the candidate makes any claims that are found to be misleading or untrue their application is simply disregarded. Among the claims to be checked are employment and education history; where relevant institutions are contacted to verify any documentation submitted and references are checked. For foreign nationals proof of their eligibility to work in the state is checked, and any identification papers such as passports or driving licenses are checked using URU document checks which verify their authenticity. In some professions there are also a series of credit checks carried out

where the ‘omnibus information providers’ (Nissenbaum 2009, p. 45) such as Experian and Axciom are consulted to check for financial information such as credit defaults. In Ireland there are now a series of strict Financial Fitness and Probity regulations which cover staff in financial and insurance institutions. In practice this means that loan defaults or bankruptcy will render people in these professions legally ineligible to hold such a job. A range of other professions such as those which involve working with children will involve a Garda vetting process as part of pre-employment screening, and other licensed professions such as security operatives will have similar Garda checks.

As well as these checks on information and documentation there are also checks on the reputation of the applicant, conducted primarily through internet searches. Searching a name, address and date of birth in any search engine can often yield results which give an idea of how the person spends their spare time and as such this practice is common in recruitment. Social network sites are a rich source of information for potential employers, yet it questionable as to how accurate a portrayal of the person can be taken from them. Pictures posted on such sites most frequently depict people on holiday, socializing or doing something unusual or fun. As such the inference of the characteristics of the person may be distorted. Yet still online identities can be used to make judgments about people which affect their lives in the offline world. In fact it is common advice given by careers guidance departments of Third level institutions that job applicants conduct searches of themselves online and where possible cleanse and sanitise their image so as to present a self that is more acceptable to potential employers (Ball 2010, p. 92). This Goffmanesque form of self presentation may merely be an online version of what happens in the offline world. In the offline situation of the job interview a candidate will invariably attempt to present the face or front that best represents the version of them self most likely to appeal to the interviewer. By cleansing their online presence the candidates are merely doing the same thing by managing the online presentation of self. This can run into problems however when it is considered that much online information is beyond the control of the person and as such can be difficult if not impossible to manage.

A seemingly common characteristic in pre-employment checking is the use of outside agencies to conduct the screening. These agencies include the omnibus information providers mentioned above, but they also include private investigations firms who offer to conduct comprehensive background checks using a variety of methods which encompass both the online and offline worlds. There is undoubtedly a massive power differential involved in employment and this is even more the case at the level of recruitment. It is legally the case that permission must be sought and granted before a background check can take place, but if permission is not granted then the application will be dismissed.

### 5.5 Psychometrics and Personality Tests

As well as an increase of checks into a candidate's personal life there is also an increase of psychological and personality tests which fall under the remit of psychometric testing. These tests range from aptitude tests which claim to measure abilities such as verbal reasoning, abstract thought or problem solving, to personality tests which purport to give an accurate account of the character of the candidate. These tests aim to find not just a person with the proper attributes necessary to do the job, but also the correct personality to fit into the working environment. While aptitude tests may well be capable of measuring certain abilities such as arithmetic, personality tests may be less accurate. In completing a personality test for a potential employer, employees are again likely to utilise Goffmanian forms of self presentation as described above which would undoubtedly distort the results. As well as being used at the recruitment stage; psychometric tests are frequently administered as part of the process of applying for promotion.

### 5.6 On the Job Surveillance

There are a number of reasons typically given to justify the surveillance of workers in the workplace. These would include monitoring productivity, evaluating performance, equitably distributing rewards and sanctions, ensuring the safety of workers and ensuring the safety and efficiency of the organisation. 'Surveillance is important because

it can identify not only those who are failing to achieve production targets but those who exceed them' (Sewell 1998, p. 405). The use of various digital and electronic technologies means that there is an ever increasing amount of data which is left over from day to day working operations. More and more professions involve the use of computers in their routine operations which means that there is usually a searchable audit trail left behind in the wake of day to day work activities. While the double entry account system and audit trails in paper form have been prevalent for hundreds of years, the use of digital equipment in contemporary work makes these audit trails far more usable as a management resource which facilitates Computer Based Performance Management (CBPM). This is because the data are easier to store, retrieve, combine, interrogate, and disseminate.

A further example can be found in the prevalence of swipe cards being used in office buildings, where access to the building and to certain parts of it once inside is dependent on the employee swiping their card in a reader. While such systems are undoubtedly in place for stated reasons of security and to protect the organisations assets; one of their by-products is that there is individualised data kept which tells when each employee came in to work, each time they went to the lavatory, how long they took for lunch and so forth. In some places these swipe cards are also used for purchasing food and beverages in the cafeteria yielding data regarding employee's dietary habits. Another technology is the RFID enabled 'active badges' (Marx 1999) which constantly emit a signature radio frequency which can be picked up by receivers in the workplace thus accounting for employees movements at all times. This data can be matched with the audit trail data generated by work conducted on computers and can give management a detailed vision of how an employee spends their day. As well as these commonplace technologies there is also a profitable market in workplace surveillance equipment such as key stroke monitors/recorders, screen grab software and filters which monitor email content for defined words. Even in jobs that take place outside the strictures of an office building such as travelling sales or deliveries there is an ever increasing capability to monitor through GPS and mobile phone technologies. The mass of data which is generated in the contemporary workplace has become part and parcel of the process of

measuring employee performance and enhancing management techniques of control over employees and the work process. This ‘omniscience’ (Wood 1998) (Marx 1999) is a central feature of contemporary computer based work and management practices.

The legal basis for workplace surveillance in Ireland is at best a grey area; while there are no explicit laws permitting or forbidding it, there are guidelines which have been drawn from other legal avenues most notably the Data Protection Acts. Surveillance is typically ordered around the principle of informed consent; employers are required to furnish employees with a policy document which details the rules for using company equipment, and any forms of workplace monitoring must be outlined there. By this reckoning covert monitoring of email is deemed to be illegal as employees would not have been given notification. Other guidelines include those which deal with the basis for monitoring; in order for monitoring to be legal it must first be shown that other avenues or methods have been exhausted. Surveillance must be proportionate, if a person is to have their work communications monitored it must be to prevent serious misuse of company time or equipment. It would be unacceptable to use the reason of minor stationary theft for example. With email monitoring there is also a legal requirement to protect the privacy of people outside of the company who correspond electronically. For this reason most work emails will have a footer at the bottom which will outline email policy which is taken to suffice that the correspondent has been adequately informed.

## 5.7 Discussion and Results

### 5.7.1 The Private Lives of Employees

The most notable and commonly repeated answer during the sections of the interviews which related to work was the response to the question: *how would you react if you found out your employer was watching you outside of work?* All respondents voiced some degree of opposition to this possibility with the most common reason being that

work life should be completely separate from family or private life with a clear distinction between the two being maintained. This separation of work and personal life was more sharply guarded by older respondents who expressed outrage at the prospect of their personal lives being monitored by their employers. This outrage was sometimes expressed in terms of a right to privacy, that such monitoring was in breach of this right and that it overstepped bounds of legality and even decency.

I: erm what would you think if you thought your employer was watching you outside of work? so if you say that, it probably wouldn't apply to you as much with the job you do but say, someone kept an eye on your Facebook account?

R: I'd go mental, I'd go absolutely mental, they have no right to, it's completely separate

I: Right, ok

R: as far as I'm concerned they have no right to that outside of work,

I: So you'd see a complete separation between your work and private life?

R: Unless your private life is getting involved in work, but even with that they would have no right to into your Facebook or whatever to see what I was doing.

I: Ok

R: As far as I'm concerned they don't anyway,

(Peter)

I: what would you think if you found out that your employer was monitoring what you do outside of work, so if they were kind of like looking at your facebook profile or

R: not happy at all, actually I'd consider taking a legal action against an employer who did that, it's completely, em it's eh completely outside the norms of I suppose decent practice and I'd imagine it's illegal, I don't know if it's not but I'd hope that it is

(Pat)

In this response we can see a strongly articulated opposition to employee lifestyle monitoring to the extent that Pat would consider legal action to prevent it. There is a moral imperative mentioned as according to Pat such monitoring is outside of decent practice, is seen as underhand or sneaky and for these reasons is unacceptable.

R: I can see already some companies that em eh some corporations are getting people to give them their Facebook information when they get hired for a job you have to give them your twitter and Facebook information so that they can log in and view what you've said on Facebook and everything else, that to me is a total infringement on your rights, I mean when you clock out at six o'clock you should be able to go home and not think about work again

I: so it's like there should be a complete separation of

R: that's exactly it yeah it's basically an invasion of, and basically it's just to see what, what you're saying about their corporation and you know the kind attitude you have to your job and everything else… so that's worrying I'd definitely be against it I mean that's, I mean there's absolutely no reason for a job to be infringing on your rights like at all

(Rory)

The Irish Congress of Trade Unions (ICTU) claimed in November 2012 that pre-employment checks had become more invasive and even included potential employees having to surrender their social networking sites passwords to recruiters. This interview however had taken place a number of months beforehand yet this practice was

mentioned by the respondent who claimed that it was relatively commonplace. Work is characterised by these few respondents as being a completely separate sphere from personal and family life; and any attempted mixing of work in the family sphere was thus characterised as an invasion. Interestingly though it seems that the opposite is also seen to be true, that any negative elements of family and personal life which affect work performance are also deemed unacceptable and worthy of remedial action. While Peter rejected employee monitoring in the strongest terms he did so with the qualifier "*Unless your private life is getting involved in work".* So arguably the separation of work and personal life can be seen to work both ways, respondents who expressed the strongest desire for work to stay out of their personal lives were the same ones who endeavoured to keep their personal lives away from their work. This can be seen most clearly in responses to questions on drug and alcohol testing which will be looked at below. Despite all respondents making the distinction between personal and professional life, there was some mention of the fact that the two can meet in the online world particularly in the process of job searching.

I: ok em what would you think if you found out your employer was em using the internet or something to keep an eye on you outside of work

R: oh I wouldn't like that at all,

I: would you think it's likely to happen

R: I've heard of people doing it, like if you apply for a job that they put your name into Facebook and check out you know if your profile is not private, I've heard of people saying that you know, don't ever put anything up on Facebook that is going to come back and bite you if you're going for a job, or something that your employer can throw back in your face like you did this or I saw this on Facebook I have heard that (Margaret)

While almost all respondents expressed similar reservations regarding employer surveillance of their personal life, a striking difference however was how some felt that it was completely their own responsibility to manage their alternate identities. As mentioned above it was the participants that make up the higher age range of the sample who voiced objections to employer monitoring of their personal lives. While younger respondents voiced similar objections they were more attuned to the fact of identity management particularly in the online context.

I: How would you feel if you found out your employer was watching you outside of work? like looking at your Facebook or

R: eh I wouldn't be too keen on it but then you see at the same time like once you're on Facebook if you're friends with somebody who is your boss which is obviously a bad idea, and likewise if you have your privacy settings set where everybody can see any thing you put up on Facebook then obviously you're not too bothered about people knowing stuff about you, but I can understand why certain employers are going online now if they have people in for an interview and they look them up on Facebook to see what they're doing and what their social life is like because if people are on there kinda blabbing about like taking drugs or getting drunk all the time then it's not gonna be something that will stand, stand to you really, it wouldn't show you to be a good character

(Harry)

I: How would you feel if you found out your employer was watching you outside of work? like looking at your Facebook accounts or anything

R: yeah, em mine does, but that's ok because we're friends at this stage, but em I would be uncomfortable because the person I am in Facebook isn't the person I am in work. you know I'd be all protests and giving out on Facebook, and whereas in work I just do my work, I'm an employee so I put on a face, and then private stuff as well like I might

have a Shakespearian poem up, and they would be like oh my God she makes me want to vomit, so I would rather not

(Anna)

The nature of situational identity is aptly described here, *"the person I am in Facebook isn't the person I am in work",* Goffman's impression management is also unwittingly but exactly reproduced *"I'm an employee so I put on a face"*. This respondent who is in her early twenties is typical of her age cohorts who were interviewed as she is quite aware of the multiple identities and roles which constitute social life. Respondents in this range were particularly savvier in managing their online identities and matching them with offline 'real world' audiences and situations. Two strategies which were spoken about for identity management between the online and offline world were limited access, and dual identities. While the fact of dual identities was acknowledged by Darren, he noted how he was in control of his personal identity outside of work particularly online. Through having a thorough understanding of online privacy settings Darren could practice a digital version of limited access to self.

I: Yeah, ehm and how would you feel if you found out your employer was looking at you outside of work? so like checking your Facebook profile for example

R: I wouldn't be bothered really, again depending on who he is or what he is or who she is or what she is, I'd have my security settings tied up

I: So the level of access to you is basically what you will allow them?

R: yeah what I allow them yeah

This same claim that there is personal responsibility for keeping personal and professional lives separate was also made by Hannah.

I: and if you found out that your employers were watching you outside of work like say they were watching your Facebook profile for example how would you feel about that

R: if it was an issue I'd be thinking, I'm thinking now that I wouldn't care but then if I think about them looking at it and thinking well that's how they view me in work then I may have an issue with it do you know, but that's up to me to keep it private and not to, you know if I don't want anyone in work to be looking at it not to have any of them in work....

I: as a friend

R: yeah yeah

I: so you think it's your responsibility

R: yeah

(Hannah)

### 5.7.2 Alternating Identities

In consuming online products and services users agree often unwittingly to lengthy statements of terms and conditions. These statements often include a clause or reference which allows the operators of the service to change the terms of use as they see fit. As well as this privacy settings are subject to constant change of which users are not always notified. These practices mean that there is a marked power differential between users and operators and it is difficult for users to know at any time exactly how 'private' any of their online actions are, this point will be taken up in detail in chapter seven. As we have seen above it is believed to be a commonplace occurrence that human resources professionals conduct searches online to supplement their knowledge of applicants. While the prevailing advice may be for job seekers to try to manage or cleanse their online identity, a different approach was uncovered during the interviews. Paul is in and out of work due to the seasonal nature of his profession and because of this finds himself

regularly applying for work. Instead of cleansing his online identity, he creates an alternative one. When using social networking sites, comment boards etc in a professional capacity Paul uses his name as normal. When using these sites in a personal capacity however Paul spells his name phonetically ie. 'Pawl'.

R: yeah you know, just in case I write something that might not go down too well with you know someone who might end up being a potential employer or something someday you know, I might be after writing alot of obscene stuff on my facebook page (Paul)

By creating dual online identities Paul has identified a strategy for managing the separate spheres of his life. As 'Paul' he can use a professional identity through sites such as linkedin.com and network with other professionals in his field while looking for work. As 'Pawl' he can use his personal identity on sites such as Facebook to tell rude jokes and to be himself. By separating the two he is strategically managing his identity and separating his personal life from his professional life. This is the best example of the savvy strategies employed by participants in the younger age cohort to actively manage their online presence.

### 5.7.3 Alcohol and Drug Testing

As is evident from above; the majority of those interviewed expressed strong reservations about the mixing of work and private life. The disclaimer of "unless your private life is getting involved in work" is particularly interesting because of the frequency of its repetition. A common refrain from the interviews was that employer intervention would be acceptable in the case of drug, alcohol, or health problems which would have to manifest themselves as lapses in work performance in order for it to warrant employer intervention. Where this happens, personal life is infringing upon the sphere of work life, and this is deemed to be unacceptable by respondents. There was a question which asked directly if it would be acceptable for an employer to demand an alcohol or drug test from their employees. The nature of the power relationship was

frequently noted and this was seen as compelling employees to undertake such tests if they were requested.

R: em I don't know eh I'd have to do it because a job is a job, you know whatever if they said you have to do this I'd have to agree to it, I wouldn't want to rock the boat jobs are scarce! (laughs)

(Margaret)

The power relationships built into the workplace make it difficult for subordinates to refuse such requests. In a time of economic recession and high unemployment such as when these interviews took place, these top down power relationships are solidified and reinforced as employees grow ever fearful of losing their jobs and being thrown to the vagaries of a difficult jobs market. This is likely to create a more compliant workforce who are less likely to "rock the boat" and more likely to agree -even grudgingly- to such demands.

The nature of drug testing in the workplace is such that denial or refusal to cooperate can be construed as having something to hide (Gilliom 1994). This sentiment was common, as was the view that even the act of being asked to take a test was related in some way to an assumption of guilt, or at least a presumption as to the lifestyle of the employee.

R: eh well I suppose on their part the assumption would be that they need to screen me for drugs which means that they are assuming that I'm taking drugs or they're guessing that I'm taking drugs, so whether that has to do with like my gender or age or whatever that kind of thing where they are making assumptions em and then I suppose if you refuse then they're gonna make the assumption that you have something to hide so you can't really win in a situation like that
(Harry)

In this instance Harry expands upon the point of an assumption of guilt that goes with a drug test and explores some the potential reasons as to why this assumption could be

made; *"whether that has to do with like my gender or age or whatever that kind of thing where they are making assumptions"*. This is an accurate description of what Gary Marx (1988, p. 219) terms 'categorical suspicion' where people are placed under suspicion and treated accordingly not because of their words or actions, but because of their belonging to a given category. In this instance the suspicious category is that of young person who are deemed to be most likely to imbibe in illegal recreational drugs. Suspect categories can be determined according to race or ethnicity, gender, age, socio-economic standing or any number of other parameters. Once a category is defined as being suspect; all people who belong to it become subject to more intensive attention from the authorities. In the present context the category may be based on age, gender and any other behavioural aspects which could make up the category of a person who is likely to abuse drugs. The concept of categorical suspicion will be explored further in chapter six, but for now it is sufficient to note how workplace drug testing comes with a complex set of assumptions even when it is claimed to operate in a random basis.

I: how would you feel if you had to complete a drug or alcohol screening in work

R: yeah it would seem a bit insulting that, 'cos I would assume that they're assuming guilt, you know, first off they don't trust if you say, though I suppose if they asked if you took illegal drugs em

I: you're unlikely to say yeah

R: yeah
(Paul)

This respondent has once more noted the unintended communicative messages associated with workplace drug testing. The assumption of guilt is described in terms of an insult and as being indicative of a lack of trust. Interestingly though this is partially withdrawn as he concedes that narrative accounts of illegal behaviour are unlikely to be reliable. This perceived distrust of narrative accounts stems from the fact that if it is in a

person's interest to lie, and if they are likely to get away with it then they are to be expected to do so, particularly if their livelihood depends on it. It is with this in mind that the testing of blood, saliva or hair for the presence of illegal drugs is seen as the only way to know for sure. 'If the content of the words can't be trusted, perhaps physical traces can be' (Andrejevic 2005, p. 480). 'The result is that government and corporate authorities no longer need to discover misbehaviour through verbal testimony or chance observation because they can cut through the human faculties of secrecy, deception or denial, look inside the body and see what the individual has been doing' (Gilliom 1994, p. 1). This faith in empirical scientific and observable reality is held because of the belief that scientific "facts" don't tell lies, don't have an interest in self- preservation and as such are more reliable than narrative explicative accounts.

Once more these two respondents have considered any assumptions that are inherent in workplace drug testing

I: ok em and how, if you were asked to complete a drug or alcohol screening in work how would you feel about that, or have you ever been asked

R: no I've never been asked, I wouldn't be happy if em there was no indication whatsoever from my performance or my conduct in work that would suggest that I would have an alleged alcohol or drug problem, I think in an extreme case and provided they've taken a lot of legal advice on it that they can, again serious grounds of suspicion for doing such a test and if its in relation to basics of even health and safety and em professional conduct during work maybe then yeah they could but not without grounds definitely not

I: and the grounds would be basically if you weren't doing your job properly or

R: yeah but I think the burden of proof would have to rest on the employer they would have to have, be able to prove serious grounds of concern that em my conduct in work em

I: merited?

R: merited such a test

(Pat)

Ireland was one of the first EU countries to legislate for workplace drug testing with the Safety Health and Welfare at Work Act 2005. The aim of this legislation was to facilitate workplace safety and avoid accidents caused by intoxication. Section 13 (b) and (c) related directly to this stating that 'An employee shall while at work,(b) ensure that he or she is not under the influence of an intoxicant to the extent that he or she is in such a state as to endanger his or her own safety, health or welfare at work or that of any other person, and (c) if reasonably required by his or her employer, submit to any appropriate, reasonable and proportionate tests for intoxicants by, or under the supervision of, a registered medical practitioner who is a competent person, as may be prescribed'. As the act is concerned with safety, there is no compulsion for testing regimes. Instead the aim of the act is to make intoxication a safety issue and to ensure managers and supervisors working in safety sensitive environments are adequately trained to identify potential lapses in safety. Research into this area is as yet quite limited Hogan et al (2006) note how the most likely workers to be tested are not necessarily those who work in job safety sensitive environments but are instead white collar workers employed by large multinational corporations. The same research explored factors likely to influence the acceptability or otherwise of testing regimes and found that the lowest acceptable form was the random test. Instead advance warning testing regimes were deemed more acceptable with the likely reason given that advance warning tests allowed those were to be tested to exercise some form of control over the process. A further finding was that if there was no obvious justification for testing –such as a dip in worker performance- then testing regimes were less likely to be accepted; this finding was echoed in the present study.

I: and how about if you were asked to complete a drug or alcohol screening in work

R: I mean if you've got nothing to worry about you've got nothing to worry about do you know what I mean if it wasn't an issue but em I think it would be a kind of an invasion as well you know I think what you do in your own time if it's not affecting your work performance then there's no reason for it

I: so you'd say well if you're doing the job well then what's the need for it

R: that's it exactly yeah

(Rory)

In the interviews there were some exceptions as to whether or not drug testing could be acceptable; these were either if you were responsible for the safety of others in a position such as a bus driver, or if standards of work noticeably dropped. The use of random testing however was almost unanimously rejected, usually for reasons of lack of trust, or its effect on employee morale.

I: ok and how would you feel if you were asked to complete a drug or alcohol screening in work?

R: ehm actually it wouldn't be too bad

I: you wouldn't mind?

R: ehm on principle I'd mind, hmm yeah no on principle I would mind 'cos it has no bearing on my, as long as my level of performance was still there, if my level of performance had slipped or gone down to a stage where it was kind of jeopardizing the whole company or the job itself, then if they asked me is this because of it, to a degree if they just wanted it willy-nilly then no I don't think I'd be happy with it but if it was because of a certain reason maybe I would be more likely to give in to it.

(Darren)

I: ok, and how would you feel if in work or in college you were asked to complete a drug or an alcohol screening?

R: it depends what you're doing, if you're working say as a doctor or nurse then.. it probably would be advisable to check that sort of, or even a pilot like that you're not on anything, if you're just working like I said in an office or whatever then being severely hungover doesn't really affect your job so.....

I: as long as you're not hurting anyone else

R: yeah it's different if you're handling medications or an aeroplane or whatever,

(Carol)

I: em how would you feel if you were asked to complete a drug or alcohol screening in work,

R: em I'd kinda think that it was unnecessary, I suppose if you were like driving for a living and they had random tests because they needed to know that you weren't under the influence or whatever I'd say fair enough but I mean the majority of it I would have thought it to be fairly unnecessary like (Harry)

Sean who was a trade union shop steward had experience of requested drug and alcohol tests for people he represented but still held similar beliefs about its acceptability in cases where it was detrimental to work performance.

I: and how would you feel if you were asked to complete a drug or alcohol test in work

R: .... I would be very wary of anybody being asked to provide a drug or alcohol sample by an employer

I: and why would you

R: because it's infringing on their personal rights, now if it was something that they had done at work yeah there's an argument for it, it would be a difficult thing and while I was shop steward I thought it was the most difficult thing to defend is being under the influence of alcohol or drugs at work and I told the guys and the women it's the one thing I won't go into the office over, you know my feelings and I won't be defending you
(Sean)

The idea of the separation of work and private life was uniform throughout the sample as was the acceptability of drug testing in instances where work performance was effected. Thus there were no correlations relating to age or profession which influenced how participants felt. As the sample here was small it is not possible to draw wider conclusions from this yet this could be a subject which would benefit from further large scale quantitative research.

### 5.7.4 Workplace CCTV

The commonly held perception of surveillance is that it relates to direct physical watching, and as such the frequency with which video cameras and direct supervision in the workplace arose during interviews was high. Most respondents were working in or had at some stage been working in an environment where there were video cameras in operation. The ostensible reason for workplace CCTV is security, to keep assets and staff members safe yet not all responses reflected this with some pointing to how they show a lack of trust in employees, and others describing function creep, where cameras installed for security are used for other purposes such as monitoring employee behaviour. The first quote given below is indicative of the most common answer given.

I: so to do with work how would you feel about having cameras in work does it bother you

R: well they do have them in there, but I mean I suppose it doesn't bother me it's all part of security do you know what I mean, you're watched by your manager all of the time

anyway so in any job that you do, so as far as work goes em it's to cover your own back as much as anyone else so it wouldn't really bother me that much that's just security issue you know

(Rory)

CCTV cameras are embedded in the discourse of safety and security, this point will be discussed in detail in chapter 6; but for now it will suffice to note the internalisation of this discourse. Areas that are covered by CCTV are believed to be safe and secure, and in terms of the workplace cameras are seen as necessary for a number of reasons. Firstly they are believed to offer security to staff; in places where cash or valuable goods are stored they are seen to offer a protection against theft and are commonly described as a deterrent to robberies. Cameras are also seen to offer a protection against internal theft, in November 2012 it was estimated that €861 million per annum was lost to business due to employee theft. (Retail Ireland 2012) CCTV systems are seen to be central to combating such thefts and as such are there to monitor staff as well as customers as both are seen as potential thieves and monitored accordingly. In the above response a telling element is evident; "*as far as work goes em it's to cover your own back as much as anyone else."* Bearing in mind the generalised suspicion in matters of employee theft this quote is evidence that surveillance systems work both ways. While employees are monitored by their managers, they also can use the monitoring systems to hold their managers to account and to account for their own behaviour if asked to do so. This point will be explored further below in the course of examining productivity metrics. A further element of the above quote is *"you're watched by your manager all of the time anyway"* which was a common response when asked about CCTV in work. By this reckoning cameras are simply a technological extension of the view of authority and are no different from personal supervision which is typical of most work environments. This idea of camera mediated supervision being an unremarkable aspect of the contemporary workplace was also enunciated by Darren.

I: ok em what about any other jobs you might have done before

R: ehm yeah, well I wouldn't have minded, the hotel trade obviously going to have cameras, and in the bar trade it's a necessity to some degree, as in you need to have cameras in the bar, you need to have cameras over the till you need to.....
(Darren)

The necessity for cameras in indoor public spaces such as bars was described by Darren and others as being for insurance reasons. In the above passage the necessity is for cameras to monitor both the patrons and the staff; *"you need to have cameras in the bar, you need to have cameras over the till"*. This monitoring and recording of all people in a given space, particularly where there is money is seen as almost universally acceptable. The only articulated problem with this was expressed in terms of an inherent lack of trust, as was typified by the response of Anna who expressed dissatisfaction at the prospect of CCTV in work,

R: I don't like the feeling of not being trusted, you know I think it should be taken for granted trust, before you know until you do something,

(Anna)

Of the fifteen interviewed only one person –belonging to the youngest age cohort- objected to workplace CCTV on the grounds that it displays a lack of trust and/or generalised suspicion. This could be explained by the seemingly common internalisation of discourses of safety and security, as is evident from Rory quoted above where workplace CCTV is described as being *"all part of security".* The purported benefits of CCTV are that they claim to offer security and safety against the myriad risks in the workplace, against these claims concerns of privacy or lack of trust are unlikely to triumph. One relatively common negative response to workplace CCTV was that it allowed for 'function creep' which is described as 'the addition of new features beyond the scope of the original project' (Lyon 2007, p. 201). In the interview responses function creep was described where cameras were seen not just as providing 'security' but being used as a management tool to supervise workers.

R: yeah, and I was working down in the filing place and I don't think they had them there, yeah I wouldn't like them, it would kind of suggest, unless they were for security like to stop someone coming in and stealing files or something like that, but I wouldn't like it if they were used to see how hard you were working or anything you know, or are you sitting down or standing up you know
(Paul)

I: and did they have video cameras in there as well?

R: they had cameras yeah,

I: and how did you feel being watched all day

R: I didn't like it you know because if you wanted to stop and ask somebody a question would it be taken that you were sort of dossing or you know I just didn't like it, I know it was for security and all of that but I didn't like the fact that em you know
(Margaret)

In these instances cameras are not seen as facilitating a safe and secure work environment but instead are seen as a constant mode of management surveillance. With Margaret, the workplace in question is a multinational retail outlet where she had worked as a cashier. As the cameras were seen to allow for the incessant gaze of management they operated in terms of structuring the outward appearance of work. Workers in customer service jobs that are under CCTV surveillance can be closely monitored to ensure that they always smile, stand correctly, wear name badges or don't waste time talking to other staff. This exact fear of function creep is that CCTV systems which are outwardly and ostensibly set up for security reasons can be used to monitor and manage staff. Sean who is a union shop steward in his workplace described a situation where this occurred.

I: how do you feel about being watched in work

*R*: em well I was used to be the shop steward there and there was, there was a couple of incidences where people were identified as not doing something at a particular time, and I had to clear up with the ------ management that those
cameras were not for employee surveillance because that was in our rule book down there you know

I: and how did they react to that

*R:* they accepted it that there was nothing they could do about it, they said no you're right

In this instance attempts at function creep were stymied with recourse to terms of employment, and the workplace in question which was strongly unionised was able to circumvent the use of cameras for anything other than security.

### 5.7.5 Computer Based Performance Management

The use of computers and digital technologies in the workplace has brought with it remarkable efficiencies and increases in productivity. A further notable factor of digitisation is that comprehensive information is generated through the routine processes of work. This wealth of information has made Computer-based Performance Management (CBPM) central to the management of many forms of work. (Ball and Wilson 2000, p. 539) Work carried out using ICT's leaves behind many traces and trails which make it possible to attribute almost every task completed to the person who carried it out. This transparency of work flows has made CBPM a dominant discourse in managing worker productivity, it allows for individual targets to be set and for performance to be judged accordingly. Gary Marx described the prerogative of this 'new managerialism' in terms of its compulsion to 'measure everything that moves' (Marx 1999). Metrics to be measured may differ from workplace to workplace depending on the job and the nature of the work, yet the results of the constant measurements are often similar. Ball (2010, p. 93) lists a number of reasons why employee surveillance can have

detrimental effects on employees; these reasons are based around ideas of informed consent so that employees know when their actions are being monitored and when their actions can have tangible effects on for example pay and promotions. Even when informed consent is maintained and employees are informed about the nature and extent of surveillance; there are still effects on both the work and the workers. Ball notes how focused surveillance on particular tasks has two likely outcomes; firstly the more a task is monitored, the more attention it will be paid even to the detriment of other work.

> 'Research finds that monitored tasks are deemed more valuable or critical than non-monitored ones, so workers will pay greater attention to the former tasks and afford greater importance to the behaviours that monitoring reinforces' (Ball 2010, p. 93).

Employee monitoring also leads to a stricter focus on the procedural and regulatory aspects of the job. Where monitoring is focused, employees act in a manner which they deem to be desirable to management; this often happens to the detriment of creativity as over surveillance breeds over compliance to procedural, regulatory and systematic modes of action. Conversely Ball also notes how overly stringent surveillance can have the exact opposite effect, where workers use 'tacit knowledge' of the systems as a form of resistance 'to subvert and manipulate the boundaries of when, where and how they are measured' (Ball 2010, p. 94). During the interviews respondents were asked about the extent of surveillance in their present or past workplaces, the question was purposefully parsed of any reference to technological surveillance so as to allow for a broader discussion on oversight and management and how they are tied in with surveillance. A further question asked about performance objectives with the aim of discovering how they were instituted, maintained and measured as well as whether or not respondents felt that such measurements were fair.

Some of those interviewed did not have specific numerical targets which measured their productivity, for example one respondent was a special needs childcare assistant, another was an orderly/porter and neither of these professions entailed any form of performance

targets or appraisals. The respondents most likely to have experienced CBPM were those who worked in the retail or financial services sector, these predominantly white-collar jobs are computer based and so are amenable to CBPM. Other professions spoke of how it was the case that while they did not have direct and articulated targets or appraisals they were monitored for quality assurance purposes and so only had such management contact when they had made a mistake or were being reprimanded.

The response to targets and their enforcement through CBPM practices was mixed, while some respondents felt that such practices limited their autonomy and forced them into behaving in certain ways, others simply saw it as part of the process.

I: Ok have you ever worked anywhere where you've had like performance objectives?

R: yeah

I : and how closely were they monitored?

R: they were monitored quite close actually, like in ------ up the road there, and that's a big thing, it's more of a big thing now that they're struggling, I don't work there now, but yeah it was all every week you would have to see what you had sold and how you sold it and all this kind of shit.

I: I didn't know they had sales targets there

R: Big time

I: and how do you feel about that level of, I mean would they keep track of what you sell every week?

R: yeah well like it puts a lot of pressure on you, you know, and then of course your self esteem is a bit shit if you don't and it's more pressure than anything pressure to, 'cos

you know, it's outside your control essentially like, if that person hasn't got money, what the fuck are you supposed to do? so it's capitalist scumbags but that's the way life, the way it is.

(Anna)

In this instance a description typical of many retail outlets is being described, workers who on the face of it are employed as cashiers or customer service representatives are measured predominantly in terms of their sales output. While public perception may be that such employees are predominantly service oriented, the reality is that they are working in sales jobs and as such are constantly having their individual sales output measured and compared with others. These practices were found in this study to be common among retail, insurance, banking and any other forms of customer facing jobs. It is evident from the passage quoted above that such practices can lead to such jobs being highly stressful as achieving such targets is seen as being outside of the control of the worker; *"it's more pressure than anything pressure to, 'cos you know, it's outside your control essentially"* In these instances work becomes a numbers game where each day is about filling a quota or reaching a target, these are measured constantly and staff often receive daily feedback from their managers.

R: you've got to make about fifteen or twenty percent on ---- a day, so you've got to be pushing it on people all the time eh you've got to kind of em you've got to try and get them to pay that extra and if you can you've to get people to buy used stuff the whole time eh because they make more money off it, (Rory)

In this instance the numbers are based on an insurance type product on which the company in question makes a high profit. The constant monitoring of this target in particular meant that this respondent was constantly focused on this particular target and was given constant updates and reminders from his manager as to how he was measuring up against it.

R: it is yeah, it is tracked, there's a kind of end of day report they do that em they'll mark it up against the, I mean the manager will be actively saying to you the whole time oh you've only got you know nought percent of ---- protection today or five percent of your ---- protection today

This deeply ingrained sales culture was also evident in two respondents who worked in banks where they were given daily, weekly, monthly and yearly 'run rates' for sales targets that they were expected to hit.

R: you would be given a target for the week, a weekly target a monthly target, a quarterly target a half yearly target and a yearly target so if you slipped on one target you would have to clamour to get up to reach the next target.

(Darren)

As with the example quoted above this led to a sharp focus on these targets and unremitting pressure was exerted on staff not just from their manager, but also from managers higher up the chain. A further element of this sales culture which was evident in retail, banking and insurance jobs was how in some instances there were computerised sales prompts built into the systems. These prompts took the form of products which were to be pitched at the customer at the point of sale, so for example in the case of banking if a customer was buying foreign currency, the computer system would prompt the operator to offer travel insurance. In some cases the operator had to input reasons as to why each product was rejected by the customer. This type of fully automatic system was the subject of complaint among its users with the lack of autonomy being the most prevalent complaint.

R: yeah they do yeah, the first thing that will come up is eh lets say you're selling a console, if you scan a PS3 console the first thing that will come up is HDMI cable and a question mark, and then it comes up make sure the customer knows that extra controllers are only thirty quid and stuff like that, and it's one element of the job I absolutely hate because it's like working in McDonalds you know, it's that American mentality that you have to keep pushing pushing and pushing the whole time ….. it's all profit, they want

you to be pushing used, and they want you to be pushing hardware attachments, an awful lot of stuff that people don't want, not that they don't want it but they don't need it in the first place you know,

(Rory)

As noted above there is nothing new about workplace oversight, monitoring or surveillance; what is new is the extent to which it is possible due to technology. In some work environments the computerisation of work flows has relegated workers to the status of operators that fit neatly into the system and have their work practices dictated to them by computer systems. The use of these systems dehumanises and alienates work as there is little staff control over the tasks they undertake and they are instead following computer based procedural work flows into which they have no input. In these types of jobs another common factor mentioned was the link between individualised and collective targets. While each member of staff had their given targets, there were also targets for each branch. The branch targets were then compared against other branches across the country with competition being encouraged.

I: and do they have targets for the shop as well as for each person

R: oh yeah they do, em there's like league tables where every shop in the region is put against each other, and every shop in the country and you're supposed to really give a shit about that, like they you know get all excited about it and you have to pretend to care. (Rory)

Service jobs are often referred to as involving emotional labour 'which is defined as the effort involved in performing emotional regulation for the purpose of complying with the interpersonal demands required in order to perform a job.' (Monaghan 2006, p. 15) This involves putting on a face for work, to be pleasant, approachable and so on for customers despite whatever happens to be going on in workers lives. From the quote above it can be seen that such forms of impression management are not solely for the benefit of customers but are also for other staff and management, "*you're supposed to*

*really give a shit about that, like they you know get all excited about it and you have to pretend to care."* The close monitoring of performance targets is also usually tied up with remuneration where rates of pay are increased according to realisation of targets as Darren who formerly worked as a financial advisor states.

R: they were more kind of expected of you but because they were commission based it's kind of if you didn't hit these targets, there was an incentive, as soon as you go over the target you're incentivised more financially as in your commission rates go up your percentage rates go up so if I didn't hit a target this year not that the boss would laugh at you but he would smile at you as if to say, yes you still made me x amount of money but now I don't have to pay you as much. (Darren)

As can be seen above there were a number of interviewees who disliked working under such conditions, this was not uniform however as Hannah who works in a telesales environment states.

R: our targets well they would be like, I mean hitting my target depended on how much I get paid you know, so like you wouldn't get sacked for not hitting them, they wouldn't be say as pressurized as in the banks, there would be enough pressure but not, not to the degree of serious sales environments you know,

I: how do you feel about, you know the amount of information they gather to measure your performance, how do you feel about that do you think it's justified or

R: well ours is very, ours is very open and closed, you've either sold it or you haven't so it's you've either sold a car policy or you haven't sold a car policy do you know what I mean so it's, our stats come up, literally it's just a report that comes up and your figure comes up and ...(Hannah)

According to Hannah such targets are fair because they are not enforced with the degree of pressure that would be found in *"serious sales environments"*. The incentive to hit

targets is positive, if a target is met bonuses are paid as opposed to some of the other negative incentives where if you don't hit the targets you will be fired or demoted. Hannah also speaks of the relative simplicity of the CBPM system she works under, *"you've either sold it or you haven't"* and this simplicity as opposed to other workplaces described which operate under percentages and run rates and so on is possibly the reason why it is acceptable to her.

### 5.7.6 The Reflected Gaze

As Hannah works in a call centre she is the most surveilled worker in the sample. As well as having sales targets monitored she has a raft of statistics such as time spent on each call, and so on. She also as is typical of call centres has each call she takes recorded, and once a month she must sit with her supervisor and listen back to a randomly selected call for purposes of 'quality control'. When asked about this element of her work she did not express any unease or reservations about her working life being recorded and permanently stored. Conversely she welcomed this as being a means by which she could be proven right in the case of customer disputes.

I: and what about, are your calls listened back to or monitored or

R: yeah

I: and how do you feel about that

R: to be honest I don't mind, it's kind of like a safety net,

I: that if someone says

R: yeah she said this or, no it's grand they can listen back to it, it doesn't always work in my favour, if you make a boo boo it's like there you know to be heard but now I have no issue with it at all because you know it's as much in my favour as the consumers

Here surveillance is not characterised as top down and authoritative, instead it is seen as a means of achieving transparency of work practices. As Hannah mentions this does not always work in her favour; if she makes mistakes they can be traced directly back to her. Yet she sees such transparency as a good thing as "*it's as much in my favour as the consumers".* This idea of surveillance being used to the advantage of those who operate under it was a recurring theme in the questions asked on workplace surveillance. Paul who was formerly employed as a delivery driver was asked about Global Positioning Systems (GPS) being used in work vans to monitor driver location. The company he had worked for did not use such systems yet surprisingly Paul expressed dissatisfaction about this.

R: uhm I had a phone alright but they couldn't keep track, I remember eh because they wouldn't give me overtime because they said drivers don't get overtime because they said some drivers used to pull in by the side of the road apparently and they assumed that all drivers would be guilty of that so any overtime they wouldn't pay it which is totally illegal, So I kind of suggested you know look if you want to put something on the van you know like a GPS tracker or something like that so you know I'm not pulling in by the side of the road you know, I want my extra eh wages you know, or the money that I'm owed (Paul)

Surveillance is not seen in this instance as an authoritative top down dictation of management to employees, instead GPS surveillance is actively sought by employees as a means of enforcing their terms of employment and being properly paid for the work that they have done. This transparency of omniscient organisations which is enabled through CBPM, and enhanced ICT systems is one which works both ways as employees can use the records to hold their employers to account. Another respondent, Harry had worked as a driver and was given a GPS system to keep track of his whereabouts.

R: I did have a company phone as well so they would have known, and if I was in one of the work vehicles that has a tracker on it as well so they can log into a website and see where the vehicle is

I: and how did you feel about that

R: I kind of thought that it was like fair enough ‘cos once your on the road I mean if you’re out and about you could be anywhere and doing anything like do you know what I mean, so they need to know that you’re getting the job done, so like once you take the job you either accept these conditions or you don’t so I would have thought that it was fair enough you know (Harry)

The use of tracking systems is seen as facilitating full transparency, jobs which involve workers being away or on the road most of the time have through the use of technology been drawn in to be subject to close managerial control and oversight. In the limited sample of workers interviewed who are employed in these jobs the reaction to this development was surprisingly positive. These reactions ranged from actually seeking such systems to be put in place as a means of proving work rates, to full acceptance *“once you take the job you either accept these conditions or you don’t so I would have thought that it was fair enough”*

## 5.8 Conclusion

The workplace is a particularly interesting social sphere to question aspects of surveillance. Differentials in power between employee and employer mean that surveillance systems are most often applied in a top down ‘take it or leave it’ style. With this being the case it would be reasonable to expect resentment and resistance on the part of those subject to such systems. This however was not the case according to those interviewed; the picture of the relationship between workers and the systems used to monitor and measure them at work is complex and multi faceted. As is evident from above, workplace surveillance engenders a culture of transparency and accountability where work is traceable to the person who carried it out. While such systems may be imposed in a top down fashion, they can be used by workers as a means of holding their employers or managers to account. The most strongly articulated opposition to

workplace surveillance was reserved for reputational monitoring which makes employees personal lives outside of work the subject of enquiry. The most commonly stated opposition to this was that there should be a clear separation of work and personal life. Once again however the picture is more nuanced and complex than is seen at first sight as the separation of the two spheres of life works both ways. While there was the unanimous assertion of work having no right to intrude upon personal life, there was also a tacit belief that personal life should not intrude in work. This was most plainly evident in the discussions on drug and alcohol testing, where a common refrain was that such testing was acceptable if there was a decrease in performance or productivity. This would seem to suggest that testing regimes in the workplace could be more acceptable to employees if they were linked to metrics of productivity. Amongst this admittedly limited sample it seems that where performance is adequate there should be no need for alcohol or drug testing. In operational terms this may not be feasible however; this is because if it were the case that testing was linked solely with poor performance, then it would be associated with punishment. The workforce as an entity is constantly in flux and changing due to natural factors such as retirement, death and the yearly entry of new workers as educational institutions turn out graduates. This changeable nature means that social norms which arise from the workplace are also fluid and changeable. With this in mind it is worth noting how workplace monitoring and surveillance can easily become normalised among younger workers and new employees. There was however no discernable difference of opinion regarding workplace surveillance which correlated with the age of the participant, such correlation could potentially be found in a quantitative study which utilised a much larger sample.

# Chapter Six

# Surveillance, Security and the State

## 6.1 Introduction

Surveillance is most commonly associated with Police work; suspect people or groups are monitored by the Police with the aim of catching them in the act of doing something illegal. As we have seen previously; this is the typical way in which surveillance is defined, with suspect groups being *physically* watched and followed. This form of surveillance is relatively commonplace; the Garda Siochana have a number of surveillance units which are focused on placing people of interest such as members of criminal gangs or terrorist organisations under watch. These units can take the form of the National Surveillance Unit, (NSU) the Organised Crime Unit (OCU) and the National Drugs Unit (NDU) to name but a few. Law enforcement has also embraced the use of the internet and other forms of networked communications as a means of investigation. The monitoring of traces discussed previously has been shown repeatedly to be a useful investigatory technique; recently a number of high profile murder cases have used such evidence decisively in proving either guilt or innocence.

The most famous of these is the Rachel O'Reilly murder case; where her husband Joe O'Reilly was proven to be lying about his whereabouts at the time of the murder. Although he had claimed to be at a bus depot in Phibsboro he was found to have been in the vicinity of his home where his wife had been murdered. It was locational data generated by his mobile telephone that was crucial in debunking his claims. The Viacom communications group triangulated a signal from a text message sent from his phone and proved that Mr O'Reilly had been on the M1 motorway at the time which placed him close to the scene of the murder. The Gardai are not alone as state actors who use such techniques; the Revenue Commissioners use surveillance techniques to investigate tax evasion and smuggling, and the Irish Army is actively used to monitor groups deemed to be a threat to the state. In practice this seems mostly to be terrorist groups such as the Real Irish Republican Army, (RIRA) or the Continuity Irish Republican Army (CIRA) which are described under the blanket description of dissident

republicans. The use of terrorism as a reason for the ramping up of surveillance measures has steadily gathered pace since the Al-Qaeda attacks on the American city of New York in September 2001. The dynamics involved in the use of insecurity as a mode of governance will be explored in detail with the aim of elucidating the manner in which fear can be profitable; both financially and politically.

Surveillance often falls across the remit of the three agencies; for example the Revenue Commissioners aim in conducting surveillance would most often be to uncover tax evasion, money laundering or smuggling. If these practices are carried out by so called criminal gangs who are involved in drug crimes then the Revenue will link up with the relevant agencies in the Garda organisation. If these activities were carried out by terrorist groups who were deemed to be a threat to the state; then the Revenue might link up with the Army. Such operations often in practise, recruit other members of society to conduct surveillance at their behest; for example telecommunications companies are legally compelled to retain data and hand it over to designated actors in certain situations. As well as this other areas of the state such as the Department of Social Welfare have been anecdotally described as using surveillance measures such as monitoring social networking sites and using data matching techniques to try and root out welfare fraud. This example is quite typical of contemporary forms of surveillance; information which is publicly available, and is often left behind in the course of contemporary interaction is sought out and used for purposes other than that which they were originally intended. This process is described by Lyon (2003, p. 95) in terms of integration or convergence; where dispersed, rhizomatic data which is held in a variety of places by a variety of actors; is gathered by agents of the state for analysis.

Information generated through routine actions such as consumption or communication can be gathered and interrogated by apparatuses of the state for diverse purposes such as law enforcement, investigations, national security, fraud reduction and so on. The use of Closed Circuit Television Systems (CCTV) as a law enforcement tool will also be looked at in detail, with particular focus on open street systems. The main findings to be presented are that there is very little in the way of knowledge as to how state

surveillance practices operate. Where there is knowledge of a type of surveillance practice it is usually due to high profile cases such as the Joe O'Reilly case mentioned above. In talking about surveillance and security there was evident a high level of internalisation of the 'I've got nothing to hide' subject position. This has the effect of defining surveillance practices as being aimed at a criminal class of 'others' and thus not effecting those who stay within the law. The use of dragnet style mass surveillance was roundly rejected by participants with the usual reason being that there should be prior suspicion before someone is placed under surveillance. In the same vein the link between surrendering privacy and gaining security was also rejected and securitarian practices were often linked to a politics of fear.

## 6.2Security and Insecurity

Security has become a prime motivation of action at the level of both the individual, and at the level of states. The Oxford English Dictionary defines security as 'the state of being free from danger or threat, the state of feeling safe, stable, and free from fear and anxiety'. This definition relates primarily to personal security, which usually relates to being secure against acts of violence or crime. While an extended taxonomy of security would take in other aspects such as economic or environmental security; the conceptual parameters to be included in this discussion primarily relate to violence and crime. The argument is that state power is on the wane in the face of globalisation and the increasing adoption of neo-liberal market based policies. In dealing with their inability to control security in terms of standards of living and welfare; states have carved a niche for themselves in the provision of personal security and safety. Security is the most common reason given for the use of wide ranging, generalised surveillance and is often part of a dualism; where it is traded off against liberty or privacy. The process of making securitisation claims will be explored with close reference to the work of Buzan and the Copenhagen School. The flip side of security is insecurity which it will be argued constitutes a central aspect of contemporary governance. Using the idea of the 'safety state' described by Beck (1986, p. 49) and the 'personal safety state' described by Baumann (2006, p. 148) it will be argued that fears of victimisation and insecurity are central components in state governance (Simon 2007).

Security is a broad and multi-faceted concept which can be invoked to cover a vast array of meanings. For example economic security could refer to the ability of a state to pay its debts and bonds just as easily as it can refer to the ability of the people living in the same state to work and pay their own bills. As stated above the element of security to be explored here relates to security against violence and crime. The key point of distinction when discussing security is that between being secure and feeling secure. The obverse which is just as important, relates to the difference between being insecure and feeling insecure. In both cases when a person or group feels secure or insecure it is enough to influence their behaviour. In the case of insecurity; if a person or group feels threatened by something -such as another person or group, a weather event or a health risk to name but a few- it rarely matters whether or not they are *actually* threatened. Instead the *feeling* of being under threat is enough to create a reaction to that supposed threat. Similarly if a person or group is under threat, but feels a sense of security; then they are unlikely to undertake any form of action which reduces the level of threat and so will be in danger.

In terms of National or State security; the work of Barry Buzan (1983) and the Copenhagen school of Security Studies has explained the process of a threat being designated as such. It is based around a threat to a referent object; this can be a state itself, but can also be parts of the territory, people or institutions. The referent object must be deemed to be under existential threat; it must be shown that the threat endangers its very existence. This threat is designated as such by securitising actors who are usually politicians, the police, the Army, or the intelligence or security services who must convince a particular audience of its veracity. The type of audience can range – depending on the claim- from an audience of public opinion, a parliament, or a supra national organisation such as the UN security council. Once a threat is accepted by the audience, it has become securitised and thus becomes the subject of emergency actions which are by their nature extraordinary. This means that usual legal procedures can be bypassed or that extra resources can be called upon. ‘An act of securitization refers to the accepted classification of certain and not other phenomena, persons or entities as existential threats requiring emergency measures’ (Emmers 2007, pp. 111-112).

Securitisation thus deals with what Agamben (2005) refers to as the 'state of exception', and it also bears close resemblance to the extra-legal elements in the conception of 'high policing' as described by Brodeur (1983).

A point to note about the securitisation thesis is that there can be variance as to who the securitising actor may be. It is not always state, legal or law enforcement agencies that are securitising actors; a range of actors including: the media, pressure groups, and even security companies can make securitising claims. In the case of private actors such as security companies making securitising claims, there can be readily apparent conflicts of interest, where securitising claims are made which just so happen to benefit the company financially. An example of this could be seen in the clamour for biometric identity cards in the USA and Britain after terrorist attacks in 2001 and 2005. By way of example Lyon notes the offer of Larry Ellison president of database company Oracle to give 'the US government free smart card software for a national ID system' (Lyon 2003, p. 72). While the software may be free; the costs of operating and maintaining the system certainly would not be. Securitisation claims made by companies who offer costly technological solutions have recently become common. In the example of biometric identity cards Grayling notes how such companies 'stand to make many billions of pounds of income from setting up the system, issuing the first tens of millions of cards, replacing the further millions lost or stolen every year…to massive profit, in perpetuity' (Grayling 2009, p. 106). Similar securitising claims can be and have been made with respect to an array of different technologies such as CCTV, data mining software or facial recognition systems to name but a few.

Another form of securitising claim can occur in the media, when the diffusion of negative stereotypes through the mass media -in what Cohen terms 'moral panics' (Cohen 1972 ) and what Altheide terms 'discourses of fear' (2003, p. 9) -can be said to have the same effect, this will be looked at in detail below. Securitising claims are not always successful; irrespective of who makes them. The most famous example of a securitising claim that was not upheld was Colin Powell's speech to the UN in 2003 which aimed to show Iraq to be a credible threat due to its possession of weapons of

mass destruction (WMD's). The securitising claims made by American and British politicians and security personnel were essentially that Iraq represented a threat to the international order and needed to be dealt with using military force. These securitisation claims were rejected by large numbers of citizens from around the world as was evident from the sizable anti-war protests. The claims were also rejected by many members of the international community who refused to sanction the invasion of Iraq leaving Britain and America to form the so called 'Coalition of the Willing' which crucially did not have the support of the UN. Despite the fact that the invasion still occurred; the failed attempt to characterise Iraq as being a credible threat to international security is a good example of a failed securitisation claim.

An elemental aspect of security is that it is never absolute; despite claims made from any organisation or institution, complete security can almost never be guaranteed. Irrespective of police numbers, sophisticated surveillance systems, vigilance of the populace or any number of security measures or factors; there is rarely such a thing as total security. By the same token however there is no such thing as total insecurity; measures undertaken to counteract risk can significantly reduce the likelihood of their occurrence. Schneier (2003) (2008) claims that security is a 'trade-off'; in order to maximise security it is necessary to balance the effectiveness of the proposed action with the costs of implementing it. Costs can include: financial costs, costs of time or convenience or even political costs such as costs to liberty, privacy or transparency (Schneier2003, 2009) (Lyon 2003) (Grayling 2009). The most obvious example is the oft quoted trade- off between privacy and security; this holds that if states are to offer their citizens adequate protections against terrorist violence, then the self same citizens must be prepared to sacrifice some of their privacy. By sanctioning state surveillance of communications, citizens are exchanging their privacy for security.

As well as costs of security, there is also what could be termed profits, or dividends as they shall be referred to here. It will usually benefit politicians in an electoral sense if they project an image of being tough on crime, or for that matter any other form of physical insecurity. Likewise if a police or security organisation makes a successful

securitising claim it will result in more power or resources being granted to them. If a security company successfully makes a securitising claim it can be because they have a particular service or product which can counteract the alleged source of insecurity. Thus 'the capital of fear can be turned to any kind of profit' (Baumann 2006, p.145) as there are positive incentives for insecurity claims to be made by a wide range of actors. The result of this however is that insecurity is to some degree a feedback loop; the more securitisation claims are made, the less secure people feel and this leads to more and more interventions with the express aim of making people feel secure. The irony however is that while the feedback loop or echo chamber of insecurity makes people feel insecure; in objective terms citizens of developed nations have never been as secure or as unlikely to encounter acts of violence (Altheide 2003, p. 9) (Baumann 2006, p. 129) (Gardner 2009) (Pinker 2011).

### 6.3 The Safety State

In his wide ranging characterisation of the 'Risk Society' Ulrich Beck (1986) traced the emergence of a new social order which was based not so much on equality through distribution of resources; but instead on prevention. 'Whereas the Utopia of equality contains a wealth of substantial and positive goals of social change, the Utopia of the risk society remains particularly negative and defensive' (Beck 1986, p. 49). Beck's argument in summary is that modern societies have become risk societies; that in their routine operation produce negative consequences which threaten vast groups of people across all divides of class and geography. 'The speeding up of modernization has produced a gulf between the world of quantifiable risk in which we think and act, and the world of non-quantifiable insecurities that we are creating' (Beck 2002, p. 40). These risks or insecurities can include ecological damage which is a by- product of industrial production. For example if a power generating plant pumps waste into the atmosphere; the air quality will deteriorate for everyone. Poisoned air does not differentiate between classes of people or geographical location; while wealthier people may have the resources to counteract some of these produced risks there is a limit to what can be achieved. Even when there are solutions to produced risks, the solutions themselves can contribute to and even amplify other risks. If energy generation is

considered once more; it can be shown that burning fossil fuels as a means of generating energy has the adverse risk effect of emitting carbon dioxide which has many detrimental effects on the environment. A method of reducing reliance on carbon dioxide emitting means of generating energy is the use of nuclear power. Yet nuclear power generation involves the production of radioactive waste which cannot be easily disposed of and causes even greater problems and risks.

The risk society thesis can be stretched to include terrorism if global inequalities are considered. While some members of the world population live in relative extravagance - and enjoy the myriad benefits of the consumer society- a more sizeable number live in poverty, with the lottery of naissance most often being the prime determinant as to who belongs to which group. The vast proportions of global resources consumed by the former are in stark contrast with the paucity of resources available to the latter, and as there is a limited pool of global resources; over consumption by the former is at the cost of the latter. Thus the poor of the earth are 'humiliated, discredited peoples who have been excluded from its fellowship' (Pamuck 2007, p. 220). The exclusion of the global poor can be thus be seen as being a major contributory factor towards terrorism; or to use Beck's terminology terrorism is a globally produced risk which contributes to the feeling of non-quantifiable insecurity. According to Beck the 'basis and motive force' of the risk society is safety, which means that 'the utopia of the risk society remains peculiarly negative and defensive' (Beck 1992, p. 49). Thus to borrow Fromm's (1941) terminology it is a 'negative' power which is exercised, because risk society is predicated on prevention rather than facilitation. It is through preventing and avoiding traumatic events such as violent crime or terrorism that the state mandates its exercise of certain types of power, and thus governance frequently occurs in these terms.

### 6.4 The Personal Safety State

Baumann (2006) notes the separation of power and politics that is a central part of what he terms negative globalisation; 'that is globalization of business, crime or terrorism, but not of political or juridical institutions able to control them' (Baumann 2006, p. 135). In Beck's risk society thesis there is also mention made of the political vacuum, as it falls

to nation states and even individuals to try and locally manage, globally produced risks. Baumann however sees the divorce of power and politics as having a further consequence which is of particular relevance here. The reduction of the effective power and legitimacy of states in the face of globalisation, liberalisation and the prevalence of market dominated societies, means that insecurity itself becomes a valuable commodity. Insecurity according to Baumann is a means of the state reclaiming some of its lost power through the claims of the personal safety state.

> An alternative legitimation of state authority… for the benefits of dutiful citizenship need[s] urgently to be found; unsurprisingly it is currently being sought in protection against dangers to *personal safety*
>
> (Baumann 2006, p. 148 italics in original)

Because the state can no longer guarantee social safety -which relates to job security, security of social standing and esteem, the ability to educate children and so forth- it focuses on personal safety. By focussing on crime committed by archetypical figures such as organised criminal gangs, terrorists or members of the generalised underclass; and by frightening citizens into a sense of generalised insecurity; the state finds a niche for itself as provider of personal safety. Waqcuant refers to this as the 'staging of security' which

> 'has the primary function of enabling leaders in office (or competing for office) to reaffirm on the cheap the capacity of the state to act when, embracing the dogmas of neo-liberalism, they unanimously preach its impotence in economic and social matters' (Wacquant 2004, p. 243).

The political dividend which can be earned by appearing tough on crime is one which is thus more often that not enthusiastically exploited by politicians. Wacquant refers to this as 'law and order pornography' where 'everyday incidents of "insecurity" are turned into a lurid media spectacle and a permanent theatre of morality' (2004, p. 243).

While the state may benefit from the dividend of insecurity; it is by no means the only actor to do so; the media and the popular culture industry in general behave similarly. This happens when sensationalised stories which stir up panic and fear among the populace are published repeatedly due to the fact that such stories sell well. Altheide (2003, p. 9) claims that fear is a core element of popular culture entertainment; whether; it takes the form of dramatised fictional stories, or news reporting which over represents particular types of crime such as murder, violence and sexual crimes. This leads to an over representation of such crime in general culture, which in turn leads to 'the pervasive communications, symbolic awareness and expectation that danger and risk are a central feature of everyday life' (Altheide 2003, p. 9). Thus the steady stream of stories of random assaults, murders or rapes increases the level of frequency to which people believe they happen.

A recent Irish example of this can be seen in the release of sex offender Larry Murphy; where the constant stream of media stories relating to him characterised his release in terms of being a generalised threat to women all over Ireland. After snatching a woman from a supermarket car park; Murphy was caught in the act of a brutal kidnapping and rape in the Wicklow Mountains. The victim's life was saved by two hunters who happened to be passing by and recognised Murphy after he fled the scene. Murphy served ten years in prison but was believed by Gardai to be involved in a number of other cases where women disappeared, an allegation that he denies. While in prison Murphy did not avail of counselling and apparently showed little remorse for his crime. As well as this the fact that he was convicted before 2001 meant that he was not bound to a post release supervision order. His release in 2010 was met with blanket media coverage, tabloid newspapers printed glossy pull out magazines outlining the actions of 'the beast of Baltinglass'. Rumours of sightings of Murphy abounded on social media sites and there was a generalised fear among sections of the population. This fear took the form of social media sites and local news outlets which reported on 'sightings' of Murphy which always turned out to be spurious. In one instance in rural Limerick and West Tipperary 'some local people are said to have stopped walking at night and even

temporarily moved home on the basis of unconfirmed reports the convicted rapist was living in the area' (Cusack 2012).

If crime were to be reported according to the frequency of its occurrence; it would be property crime such as burglaries or petty thefts which would be most prominent and not 'gangland' crime, violence or sexual assaults which are a staple of both news reporting and fictionalised output. The repetition of such stories in the news media can take the form of campaigns in certain sections of the press which aim for changes such as in law or sentencing.

The over representation of particular types of crime has adverse effects on feelings of personal safety; it leads to generalised fears which in turn leads to calls to action to remedy the "problem" of such crime. According to Altheide such fear 'makes us more compliant in seeking help or being "rescued" from formal agents of social control' (2003, p. 22). This compliance in the face of generalised fear can be a motive force in the passage of laws aimed at tackling the perceived sources of generalised insecurity, whether they are terrorists, organised criminals, sex offenders or any of the 'folk devils' (Cohen 1972) of the time. It may be overly simplistic to lay the blame for insecurity as a form of governance solely at the door of either the media or political or state actors; in either case they could justifiably argue that they are merely giving the people what they want. There is a relatively complex interaction between media reporting, public perceptions and official reactions. The result however is that feelings of insecurity are amplified and exploited by a range of actors. As mentioned above the dividend of insecurity can differ according to who is making the security claim. If it is a security company then it can be a financial motive as they can offer a product which claims to counteract the alleged threat. If it is a political actor then it can often take the form of increased powers such as powers of surveillance, increased periods of detention or increased powers to disrupt protests. These increased powers often in practise involve a '*decoupling* of fear inspired actions from the existential tremors that generated the fears that inspired them' (Baumann 2006, p. 133 italics in original). This decoupling involves the focusing of attention on sources of anxiety or insecurity which are irrelevant but

visible so that the impression of something being done can be felt. Beck describes this in terms of being the 'hidden central issue in world risk society … *how to feign control over the uncontrollable*' (Beck 2002, p. 41 italics in original). While the impression of something being done can for a time alleviate feelings of insecurity; these feelings will inevitably return as the decoupling means that the true sources of insecurity are seldom addressed.

## 6.5 Discussion and Results

### 6.5.1 Surveillance as Security?

During the interviews the subject of security was often one of the starting points of conversation; this is because surveillance is so closely linked in common consciousness with law enforcement and the operation of the security services. As policing and security operations have become increasingly intelligence led; the contested dichotomy between privacy and security has gained prominence. The common argument is that in order for safety and security to be maintained, it is necessary for security services to increase their monitoring of private communications, financial transactions, and internet traffic and so on. 'Security technologies have proliferated, and with them two central beliefs; one, the idea that "maximum security" is a desirable goal; and two, that it can be pursued using these increasingly available techniques that are on the market' (Lyon 2003, p. 46). This contention raises complaints from civil libertarians and privacy activists who characterise it as a cynical ploy of states and security services to ratchet up popular fears as a means of consolidating their own power. As noted above others characterise it in terms of the state using insecurity as a means of asserting power, legitimacy and relevance against the backdrop of its waning powers in the face of neoliberalism and globalisation (Altheide 2003) (Baumann 2006) (Wacquant 2004). This dichotomy of privacy versus security was directly addressed in the interviews in the form of a question which asked; would you be prepared to give up some of your privacy if you were told it would make the country safer?

A small number of responses were positive to this question, and in these examples there was usually recourse to the 'nothing to hide' discursive repertoire.

R: yeah well I would, well to a certain extent I don't think, like if I was walking down the street I wouldn't have much to hide em so I wouldn't mind it and I don't think I'd be doing anything that if it was presented to me later that I would feel bad about em you know, like yeah (Paul)

In this particular instance; it was not data based surveillance which the respondent was referring to. Instead he was talking about direct surveillance or video surveillance as is evident in the phrase "*if I was walking down the street*". Further respondents who replied positively to this question added qualifying statements such as:

R: In theory yes, but in practice, in theory it sounds great but in practice it falls on whoever has that information to use it in a, in a scrupulous fashion (Darren)

So theoretically Darren has no problem with data collection being used as a security enhancing methodology; but states that in practice it falls on those who collect and keep such data to use it legitimately and within legal parameters. With reference to the relevant aspects of surveillance legislation; Irish law has not written in effective oversights which are adequate to ensure transparency and that the information is used in a "scrupulous" fashion. When talking about CCTV Darren stated that he was happy for it to be used as long as it was to be operated by a trusted organization such as the Gardai. He explicitly stated that such power to monitor should be a monopoly power and that private actors should be forbidden from doing so as they could not be trusted.

Others were against the privacy/security dichotomy for a number of reasons. The first was similar enough to Darren and his assertion of information being used in a scrupulous fashion. Whereas Darren claimed that it could happen theoretically speaking Margaret disagreed.

I: Ok and if you were told that em giving up some of your privacy would make the country safer would you happy enough to go along with it?
R: Yeah if it was going to make the country safer I probably would yeah
I: So if it was stuff say like eh I dunno maybe organized crime maybe that if the police were allowed
R: like take your fingerprints and rule you out of a... is that what you mean?
I: yeah or even if em, if the police say were investigating organized crime or terrorism and they thought that by doing a sweep of email messages sent that they could catch people, would you think that would be ok if they were reading yours as well?
R: mmm I don't know now that you say it mmm no because I think people in power can eh can ... you'll always get one bad egg in any organization I think and I think people in power if they can use that then they could use for there own gains like your financial details or your banking details, so even though they would be the police mmm no I don't think I would be happy with them being able to do a sweep of emails now that you say it. *(*Margaret*)*

To add a modicum of contextualisation; this conversation took place at a time when the News of the World phone hacking scandal was in the news. The phone hacking scandal occurred in Britain it was revealed that tabloid newspapers –particularly the News of the World- had been illegally accessing the voice mails of people they were writing stories about. The tipping point came about when it transpired that News of the World Journalists had hacked the phone of missing school girl Millie Dowler. This led to the setting up of the Leveson Inquiry which investigated press ethics, phone hacking and allegations of tabloid employees bribing public officials. This meant that information leaks from supposedly reputable sources such as The Metropolitan Police were coming to light as was evidence which linked sharp practices by tabloid journalists with police officers who were selling confidential information. With this in mind it is interesting to note the assertion that "*you'll always get one bad egg in any organization"*. The background of the phone hacking scandal showed that where valuable information is obtained in the course of duty, there is often a temptation for someone to benefit

financially. What is essential to this understanding is that it is not the institutions themselves which are inefficient or corrupt; but individuals within them, or the "*one bad egg".* Yet such institutions are only as trustworthy as their weakest link and for this reason cannot be trusted with such sweeping powers. A flaw in this logic however; is that it behoves institutions who carry such information to have robust systems of accountability in place. These should limit the abilities of the "*bad egg"* to carry out illegal deeds. Thus it is not the individual but the institutional actor which should shoulder the blame due to failures of oversight and regulation which are institutional responsibilities.

Once more, legal regulation is the place where such systems of oversight are instituted and maintained; and laws pertaining to surveillance in Ireland are arguably lacking in such effective controls. There was also direct mention of data leakage within Irish institutions which demonstrated a similar point but placed the blame on the institution.

R: examples that have come out in the media in like em, em personnel within the revenue commissioners handing out information to private firms,
I: mmhmm
R: on peoples tax records and stuff and em and certainly no sanctions being taken seems to suggest that the state doesn't treat the protection of individuals private information as something, as something that should be sacrosanct and they seem quite willing to, whether possibly unofficially eh flog it to the highest bidder (Pat)

In this instance; while it is "*personnel within the revenue commissioners"* who allegedly sold data illegally, Pat blames the institution on the grounds that *"no sanctions have been taken".* Pat also claims that "*they"* seem quite willing to sell data which implies the institution itself rather than any rogue individual operators within it.

The most common response to the question of being prepared to swap security for privacy was to reject it. The reasons for rejection differed however; and ranged from

rejecting the efficacy of such actions, to expressing distrust of the organizations involved.

I: mm ok and eh would you be prepared to give up some of what you value as being privacy for security reasons, so if you were told like you mentioned a threat to the state, be it terrorism or organised crime, would you be prepared to give up some privacy if you were told we could stop this

R: no because I don't, I wouldn't see the privacy of an individual as having anything to do with eh monitoring terrorists or anything like that I think that there's definitely a history of monitoring terrorist groups outside of interfering with your average joe soap on the street you would have had it in the North where both sides the loyalists and the nationalists would have had their groups infiltrated by various people and that, and I'm sure the whole phone tapping thing and that but I'm sure that em I don't see how me giving up any of my privacy could make any difference into monitoring someone else, I mean I don't see how me allowing someone to see my photos on Facebook could lead to the capture of em..... Osama Bin Laden or whoever do ya know, (Sean)

This view explicitly rejects the premise of pervasive surveillance as a means of policing terrorism. The paradigm of monitoring all and sundry with the aim of rooting out deviant subcategories is rejected, and there is a distinct 'othering' of terrorists. Othering 'is part of a social process whereby a dominant group defines into existence an inferior group' (Altheide 2003 p18). This takes the form of a dichotomy of "*your average Joe Soap"* who shouldn't be bothered by surveillance, as opposed to the terrorist "*Osama Bin Laden or whoever".* The example cited of Northern Ireland where there was "*a history of monitoring terrorist groups outside of interfering with your average joe soap on the street"* may be an erroneous view of historical anti-terrorist operations in Northern Ireland. Yet the underlying theme to be read from it; is that methods of policing and preventing terrorism should be focused and limited to those upon whom reasonable suspicion falls. Once more this is a rejection of the generalised suspicion that is evident in dragnet style pervasive surveillance which has become a central part of the policing

and security repertoire. Proponents of such methods can justifiably point to the fact that terrorism by its nature is often conducted by people who may fall outside the radar of the security services. As such it can be difficult to spot them which leads to the justification of generalised searches. As well as this the grounds for reasonable suspicion have to be decided upon, and these decisions are made according to information gathered through generalised surveillance.

The efficacy of generalised surveillance as a means of policing was commonly questioned during the interviews. This is evident from Sean's quote above where he states:
"I don't see how me giving up any of my privacy could make any difference into monitoring someone else, I mean I don't see how me allowing someone to see my photos on Facebook could lead to the capture of em..... Osama Bin Laden or whoever do ya know"

The link between surrendering privacy and gaining security is seen as tenuous; there is no plausible reason or explanation given as to how security and privacy are interlinked. This view is shared by Hannah:

I: em yeah and if you were told that em like at the minute say organised crime is sort of a big issue if you were told that if the state were allowed kind of, if you were told that if you gave up some of your privacy that if the state was allowed look more through your personal records or at your internet and stuff like that that it would stop organised crime would you be happy enough to let that happen or

R: no I don't think so, no I don't necessarily think that's the way to stop organised crime em I don't see how that would benefit that at all to be honest with you

While common discourse relating to privacy and security may claim that the two are odds; there was no reason forthcoming among the interviewees which validated the linkage. This meant that there was common use of the argument that mass surveillance

methods are ineffective and so illegitimate. This line of argument took a stronger turn among others who claimed that terrorism or organised crime are exaggerated and used to frighten citizens into surrendering civil rights. This line of argument states that fear is intentionally ratcheted up with the aim of increasing the powers of the state.

I:if you were told that em if you gave up some of your privacy that they could stop terrorism internationally or that they could combat organised crime or something like that would you be prepared to do it

R: probably not (laughs)

I: and what would be the reasons

R: eh I dunno like I'd, I'd be very sceptical about anything that governments would be telling you about terrorism and all this kind of thing I think that allot of times it's basically they kind of hang that over your head as a threat as a way of kind of scaring you into giving up some of your rights, when it's really like that, they're not gonna do anything unless it's beneficial to them so I think that really they're using it as a way of like taking away more of your rights so that they can make decisions without having to consult you (Harry)

The scepticism relating to official discourses on terrorism or organised crime was also described by Rory:

I: if you were told that giving up some of your privacy would make the country more secure and prevent organized crime and stuff like that

R: yeah but then if you go back to 1984 again I mean it's a slippery slope it might start off there, it might start off with em terrorism like and then it's like oh we need to check your private communications on Facebook and twitter because of say drug dealers, you

know to do with fighting the war on drugs or anything you know they'll make up any excuse

I: yeah

R: I mean once the terrorism thing runs out there's going to be just one thing after another it's a slippery slope you start there and it's just, I wouldn't be in favour of anything like that I've no reason to be investigated so, (pause) I mean there's no evidence there,

This discursive formation is similar to Baumann's (2003, p. 148) notion of the 'personal safety state' as described above; according to which the drive towards personal safety is a result of the dwindling powers of the state. While the idea that fear and insecurity are tactically used by states to increase their own powers was mentioned on a number of occasions; surprisingly the role of the media in this process was only mentioned once.

R: eh I suppose the attempt to drum up, I suppose more international media than say in Irish media or local media, to drum up the need for this to make people think that they'd be sort of better off when it's in and I'd even feel that way myself sometimes (Paul)

The most interesting element of this is the assertion that "*I'd even feel that way myself sometimes"*; even though the process of making security claims is acknowledged, so is the fact that such claims occasionally work. Even though Paul is aware of the processes involved, and the fact that securitisation claims are often exaggerated if not plain spurious; he admits to the feelings of insecurity they engender, and furthermore admits to feeling *"better off"* when measures are taken to supposedly counteract the insecurity. Any other responses which mentioned this did not admit to feelings of either: insecurity as a response to a threat, or security in response to measures taken to counteract a threat. Instead the common response was that which is characterized by Andrejevic (2005, p. 479) (2007, p. 251) as 'savvy scepticism' or to put it slightly differently, a sense of knowing cynicism. This is where respondents claimed to not be affected by insecurity

claims as the knowledge of the process grants a sense of inoculation. By knowing that insecurity claims are used to gain the varying kinds of dividends, respondents claim to be immune to the fears aroused and sceptical of the claims made.

### 6.5.2 Automatic Number Plate Recognition

As noted above when discussing CCTV systems; the use of automatic number plate recognition (ANPR) cameras by the Garda traffic corps formed part of the interview. A core feature of ANPR systems is that they gather and store a number of pieces of data in the course of their operation. While ostensibly ANPR systems are used to police traffic offences such as non-payment of motor tax or speeding; they also keep records of passing cars, even if they are legally compliant. This amounts to the –perhaps unintended- consequence of a register of movement; whereby each time a motorist passes a Garda traffic corps car, or a roadside safety van, their registration is read and a record of the location and time is stored. This de facto register of movement which is held and accessible by a national police force has not been the subject of much public discussion in Ireland. One of the vignettes used in the interviews made the operation of ANPR clear and asked for the opinion of participants, the vignette which describes the workings of the ANPR system is as follows:

Sean left home to go to work, as he drove towards town he drove past a Garda traffic corps car which recorded his registration, his car tax situation, the direction he was traveling and the time

After having this vignette read to them; participants were asked what they thought of this. The most common initial response characterized the system in terms of operability and efficiency for the policing of motor tax offences.

R: it’s illegal to be taxed, I mean to not have tax on the road when you’re driving the car then guards have to like you know find out if people are dodging it or whatever and that it saves time compared to stopping and looking at every, given the amount of motorists on the road now (Carol)

R: uh yeah I suppose the road tax is going to benefit people, so it is good that everybody pays it, I suppose the more people pay it the less it's gonna increase by anyway

I : yeah

R: so I wouldn't have any problem with that anyway

(Paul)

In these cases car tax is seen as necessary and beneficial to everyone; tax is thus characterised in terms of a communal resource, where the more people pay in, the greater the benefit to all. This is through either having a larger fund to maintain roads, or by way of there not being increases in the rate if everybody pays. In these terms; policing car tax evasion is seen as important and ANPR is seen as a rational means of ensuring compliance with taxation and of aiding and facilitating operations of the Gardai. A further response given was that it could not be in breach of privacy because the ANPR system only captures information that is publicly available anyway.

R: em I wouldn't think it's particularly been invaded because I mean anyone standing on the side of the street could have more or less picked up that kind of information (Harry)

In this case the information gathered by ANPR is seen as the same as that which could be seen by *anyone standing on the side of the street*. In these terms any information that is this visible cannot be classed as being private; and so ANPR is not seen as being invasive. The key point which is missed here however is that of memory. While such data could be gleaned from anyone in the vicinity, it is unlikely that it would be remembered. The ANPR system facilitates a register which remembers such data and renders it available for future searches.

R: if he was within the law, I don't think his privacy was, like I mean the number of his car is already going to be on public record in the registration office or whatever (Sean)

The objections that were made to the ANPR system were that it operated a form of generalised suspicion. Such systems according to this logic treat everyone as deviants or criminals and don't distinguish between those who obey the law and those in breach of it. Instead they operate in a dragnet style fashion by subjecting everyone to the gaze of authority in the hope of sifting out some for further attention. In the process of doing this however those who have broken no law are recorded and this fact raised objections.

R*:* if he wasn't speeding then he shouldn't have been recorded, you know (Margaret)

R: unless they're investigating him for suspected criminal activity they have no right to obtain that information from him, from just driving from his house to work or just driving on any road they have no right to that information (Pat)

The follow up question asked participants if they thought such information should be kept and if so; should the Gardai have access to it. This question raised further objections; the most common of which followed along the lines of generalised suspicion seen above.

R: it should be looked at immediately and if there's no, nothing untoward there then it should be gone, it shouldn't be kept for any length of time after that, especially when you mention speed and his tax and stuff, if that's all in check at the time then that should be it, there's no reason to keep it.(Darren)

This view states that policing the roads is important, and as such ANPR is a useful tool to do so. Operationally speaking it is in the interests of the Gardai to hold such data for as long as possible on the off chance that it will be useful in future operations. The problem once more is that it is a de facto register of movement as well as an algorithmic system. The car registration is linked via database to the owner which will give details of address, age, possible past offences, and so on. If the driver has been convicted of a

crime in the past, or even if he or she has been flagged as potentially being or associating with criminals, then the net result will be increased attention from law enforcement. With respect to past convictions; this can mean that the foundation of penal policy which is that a debt to society is paid when punishment is carried out has changed. Instead a person's past will always be present, this may to some degree have always been the case as those who have committed crimes in the past will be known by their victims, certain police officials, and sometimes members of the general public. This knowledge however was linked to human memory, or paper file based institutional memory and as such was likely to fade over time. The use of digital databases increases the likelihood that past indiscretions will follow someone through the course of their life. In the case of ANPR the example of a youthful indiscretion of being caught in possession of illegal drugs could feasibly lead to a lengthy period of being stopped and searched by Police. This would mean that labelling would occur, where past behaviour determines present and future treatment; in this example being caught breaking the law once feeds an assumption that a person is a law breaker and they are constantly treated as such when they come into contact with the police.

### 6.5.3 Transparency and Trust

A further aspect of the responses to these questions which related to security and policing was that of trust and transparency; the common refrain of 'I've got nothing to hide' was particularly evident in these responses. In fact having nothing to hide meant that security based surveillance was welcomed as facilitating safety and participating in solving and preventing crime.

R: No, I don't think that there's anything wrong with that, I know others would be sitting here thinking it's disgraceful,

I: do you think law enforcement agencies should have access to such information?

R: like that information, yes

I: and how long do you think they should be allowed keep it for? should they be allowed keep it indefinitely once they have it?

R: Yeah, well they are law enforcement agencies, I'm assuming they are only going to use it for law enforcement purposes. Maybe their not, but then again I'm trusting so (Anna)

R: well I think it's a kind of thing like where because it's the, the guards are keeping it you'd kinda imagine it to be safe
I: mm
R: em I think I'd really have a problem with it if it was to kinda get out, because obviously if they're kind of recording your movements and those vans are keeping a record of every time they see you then they can kind of trace and track where you're going, you know, like where you're making a habit of going at the weekends and you're in a certain place every Saturday or that kind of thing, I mean I think, as far as the Guards having that kind of information goes, I mean I think that kind of information is useful in the case where they're trying to track criminals or anything like that, they kind of know a certain few people's whereabouts and their movements, but I'd imagine that like on the whole that they probably wouldn't be bothered with most peoples like
(Harry)

There is a high level of trust in the Gardai evident in these two responses. This trust is tied up with the assumption that any information gathered will only be for operational use; "*I'm assuming they are only going to use it for law enforcement purposes"*. The trust is also invested in the institution of the Garda Siochana "*because it's the, the guards are keeping it you'd kinda imagine it to be safe".* While such trust may well be warranted it is the case that any organisation or institution can be liable to leaks (see above). It is unclear exactly what the period of retention for ANPR data is, just as it is unclear what the terms of access are, attempts by the author to find out about how such data are kept and used was unsuccessful (see Appendices). As with all institutions that deal with sensitive data there is a need for robust systems of accountability and restricted

access. Another interesting aspect here is that of obscurity in abundance which is described by Harry:

"they kind of know a certain few people's whereabouts and their movements, but I'd imagine that like on the whole that they probably wouldn't be bothered with most peoples like"

The crux of this argument is that if everyone is monitored and their movements tracked; then there is such an abundance of information that it becomes difficult for people to be singled out. This means that aside from those who are the subjects of focused attention, the rest can hide in plain sight; that just because the information is gathered doesn't mean that it will be looked at. If this is the case then information gathering by any of the security services should only cause concern to those who are likely to become subjects of focused attention. Once more this way of thinking reverts to the nothing to hide nothing to fear argument. As well as this if it is the case that most of the information gathered will never be used then it begs the question as to why it is gathered in the first place. The answer to this is that information is gathered indiscriminately, and kept on the off chance that it will be useful in future. This is the case across the full spectrum of institutions and actors, whether it's a credit card company, a police force or a hospital, the fact that data is stored for future use –potential or otherwise- has become the norm.

Surveillance and information gathering was characterised in other contexts as working both ways, for example workplace surveillance was occasionally characterised as holding employers to account just as much as employees. In much the same vein, security or policing based surveillance was seen as a means of proving compliance and adherence to the law. Once more this is an extension of the nothing to hide nothing to fear position:

R: Guards are there to do a job, so they are obviously recording, recording the number plate, in case you're speeding, recording the tax, to make sure it's in date, if it's all in

date nothing will be done about it, but if he is speeding, like any camera catches the number plate, if he is speeding he is breaking the law (pauses)

I: so he's fair game

R: he's fair game as far as I'm concerned, if you've nothing to hide you shouldn't have no problem with it,

I: Ok, and what would you think of that information being kept? so like say if Sean, 5 years later was accused of something, and the Guards retrieved that information and said oh well we can place you at such a place at such a time?

R: well I wouldn't have a real problem with that either, a similar situation happened to me, I suppose a little bit similar, we had got rid of one of the cars, about 2 or 3 years ago, and I got a letter, a summons, in the mail about 9 months after I had the car saying like a €500 fine, your car was blocking an entrance in Tramore, and I was like what? right ok and I looked and it was the reg of the old car, so I rang up the Guards there and I was like sorry mate but I haven't been in Tramore since I was 10 years old, and I sold that car 9 months ago. And he said oh well do you have all the details and everything and I said no I sold it fair and square, and I told him who I sold it too and everything, that should have been sorted out ages ago. (and he said) Right ok, let me look into and I'll get back to you. He looked into it and he got back to me. Yeah that's no problem don't worry about that, apologies for the inconvenience, its all been sorted now. So (pauses) I can't see the harm in peoples movements being kept if there not doing anything wrong.

I: So essentially if you're not up to anything bad, you should have nothing to fear?

R: Yeah pretty much, if a Guard said to me, we have pretty much all of your details on file here, I'd say that's fine, sure I'm sure that will come in handy some time. I wouldn't have a problem with it. (Peter)

While this conversation once more has recourse to the nothing to hide nothing to fear subject position, it extends it to include its two way nature. If someone has nothing to fear then they can be seen to welcome surveillance measures which they feel will grant them security. As well as this however it can be said that someone with nothing to hide can use surveillance measures to their own advantage. In the passage above Peter describes by way of example an incident where he received a fine notice for a car he had sold. The fact that there was an audit trail which showed him to have sold the car meant that he could easily dismiss the fine and be proven in the right. Thus the data trail worked to his advantage in this instance and led to him welcoming further measures of surveillance as they were also characterised as working in his favour as is evident in the statement: *if a Guard said to me, we have pretty much all of your details on file here, I'd say that's fine, sure I'm sure that will come in handy some time.*

An aspect of concern raised by two participants about data gathering and storage was that of its potential to be disclosed and used for "policing" deeds that may be immoral but are not illegal. Writing about an incident in Coventry in Britain where a middle aged lady -later named as Mary Bale- was caught on camera putting a cat into a bin; Fraser (2011) describes how norms have come to be policed across the internet. In the case of Bale –or the cat bin lady as she is infamously known- her crime was inexplicable but minor. By putting a cat into a bin she was committing an act of animal cruelty which would have earned a penalty no more severe than a small fine. Yet when the video of her actions went viral across the internet she was subject to a very public shaming which had consequences which went far beyond any punishment which could be legitimately meted out. The barrage of criticism and public vilification led to her being placed for a time under police protection, diagnosed with depression and ultimately having to resign her job of twenty-seven years (Fraser 2011, p. 9). In this case the public policing of norms administered harsher punishments than would have been possible had it been legal sanctions taken. The fact of increased transparency, visibility and monitoring of movement means that actions which are not illegal but may contravene formal or informal social norms are subject to sanction. As is evident in the case of Mary Bale the

sanctions which are carried out by the public at large for seemingly minor transgressions can be severe and life altering. When the vignette describing ANPR was read; two separate participants mentioned the policing of norms or morals.

I: do you think there should be any limits put on how that information should be used, like if the guards were going to keep it and say well this fella has an alibi but we can place him on this road at this time
R: well I suppose if he has done something wrong then I think it's good that he gets caught
I: it makes it easier to catch them I suppose
R: yeah and em maybe if he was doing something that was morally wrong but not illegal, like maybe if he was banging someone behind his wife's back or something you know, he should be entitled to, I suppose it depends on what they do with the information as well (Paul)

R: if you're just going to work and going about your business and they're able to check your tax situation and what time you're leaving I mean what if someone was having an affair? you know or something like that, that you're being watched like that (Margaret)

In both instances the example of marital infidelity is used, while this is not illegal or subject to criminal sanction it is normatively unacceptable. As in the case with Mary Bale; sanctions for normative transgressions- which are most often administered by a generalised community- can be more severe than sanctions officially administered. The point which is made by both participants above is that surveillance can limit the room which gives people the freedom to undertake such actions.

### 6.5.4 CCTV

"You know, the courts might not work anymore, but as long as everybody is videotaping everyone else, justice will be done." Marge Simpson

Closed Circuit Television Camera (CCTV) systems have become increasingly popular as a measure of combating a number of criminal problems which fall under the rubric of anti-social behaviour; including begging, vandalism theft, violent assaults and other forms of 'public order' problems. In businesses and public buildings; such systems are installed to protect assets and staff as well as being a means by which staff can be monitored. Such systems are often necessary for insurance purposes; where property owners have cameras trained on public spaces so that in the event of an accident or injury they can be protected against liability. CCTV systems have also become popular in outdoor public spaces such as in town centres for the stated purpose of eradicating violent or anti social behaviour. At present there are twenty seven open street CCTV systems in operation in Ireland. These systems are in operation in almost all major towns and cities and are usually operated in partnerships between the Gardai and the relevant local council. On the face of it, such systems represent a common sense solution to such problems. If there is a recurring problem in a particular place at a particular time; then video surveillance will capture evidence which will capture evidence. When convictions are brought, public knowledge of the CCTV systems will deter others from performing any such acts in that place in future. According to this logic; deterrence will make public areas which are covered by CCTV safe, and will encourage them to be used as zones of consumption and leisure where people will not be bothered by proscribed anti-social behaviours and will thus feel safe enough to use these spaces. This logic is evident in the 2009 report of the Canadian Surveillance Camera Awareness Network (SCAN) which offers three factors which influence the decision to install CCTV systems in public areas. These are; that they can be used to deter crime, detect instances of crime while aiding police investigations as a means of gathering evidence, and finally that they increase public perceptions of safety (SCAN 2009, p. 14).

Common discourses around CCTV systems make the dual claims that they act as a deterrent to potential violators, and they are useful as a means of gathering evidence after the fact. Indeed the Garda Siochana CCTV policy states that 'Garda Crime Prevention Officers normally recommend the installation of a CCTV system as part of a series of recommendations generally intended to prevent or detect crime' (ibid p. 1).

These views state that once an area is covered by CCTV it should be safe; as potential attackers will know that they are under watch and will act accordingly. Such views hold that in such areas if a problem is identified the system operator can call in assistance to intervene and so the gaze of police authorities is held to be constant and pervasive. Such pervasive policing is thought to foster feelings of security and safety, where people feel safe in areas where CCTV is in operation. In practice however CCTV systems are more often used after the fact to identify offenders and are of limited use as a means of pervasive policing due to any number of factors such as response times of police or even whether or not there are operators actually watching the screens. The claims made by proponents of CCTV particularly relating to feelings of safety and security were explicitly examined in these interviews.

The stakeholders involved in public area CCTV systems often have different aims and uses for it. Lett (2002, p. 11) notes how Police use them primarily as an investigative tool to gather evidence after the fact of a crime. Businesses use them in the hope of deterrence; that theft or any other petty forms of crime can be dissuaded through the close monitoring of their premises. Finally political and civic leaders see CCTV in terms of their use as a mode of gentrification of urban spaces, which will encourage inward investment and tourism, as areas that are seen to be safe and secure are suitable as zones of consumption. CCTV has thus been described as a 'silver bullet' (The Guardian 1 Nov 2007) which can be used to solve a myriad of complex social problems; the proliferation of CCTV has also led to it being referred to as the 'fifth utility' (Graham 2002, p. 237). The spread of CCTV systems can also be partially explained by economies of scale; 'once CCTV systems are installed, their logic is inevitably expansionary' (Graham 2002, p. 238). A common complaint regarding CCTV is that of displacement; if a camera is monitoring an area, then any illegal activity will be displaced away from there to somewhere that is not being watched. While the initial cost of installing a system can be high, the cost of expanding it is comparably lower and as fear of displacement takes hold the logic of expansion sets in.

The differing aims of the various actors described above do have a common denominator; the setting up of video surveillance and the motives behind it are emblematic of a new conception of urban space. This sees cities as zones of consumption or tourist destinations; described by Sassen (1996, p. 635) as 'urban glamour zones' or by Parenti (2000, p. 96) as 'theme parks'. Urban spaces have been transformed from being 'synonymous with filth lawlessness and danger' to being of 'renewed economic and cultural importance as sites of accumulation, speculation and innovative profit making' (Parenti 1999, p. 88). Central to the success or failure of these zones is the perception of safety of those who are allowed to inhabit them. CCTV has thus been utilised as a means of 'ordering' public spaces, (Walby 2005, p. 189) making them more amenable as places of consumption through the monitoring and exclusion of deviant categories of 'flawed consumers' (Baumann 2005, p. 38) or 'urban outcasts' (Wacquant 2008, p. 1). These spaces 'are tamed, sanitized, guaranteed to come free of dangerous ingredients' (Baumann 2000, p. 99) through the 'anthropoemic' (Baumann 2000, p. 99) strategies of identification and expulsion of those who do not belong; namely the poor or those who do not have the financial means to partake in consumption. CCTV can thus be thought of as an outward manifestation of the process by which urban public space has become commercialized under the auspices of neo-liberal urban renewal (Coleman 2004). Urban spaces have become commercialised and policed in a manner similar to shopping centres where normative judgements of worth based on factors as trivial or arbitrary as the type of shoes (Walby 2005, p. 195) or clothes (Norris and Armstrong 1999, p. 165) worn by a person can be deciding factors as to whether or not a person is allowed entry; and if they are allowed entry whether or not they receive attention from security staff, Police and CCTV systems.

While open air CCTV systems have been increasingly utilised over the past twenty years there has been scant attention paid to their efficacy as a mode of reducing crime. As outlined above these systems represent a seemingly common sense solution to street crimes against property and persons. Yet international studies have failed to note a clear link between CCTV use and reductions in crime. Gill and Spriggs (2005) claim that CCTV had little if any effect on crime apart from particular examples such as car parks

where vehicle theft and vandalism could take place. In such spaces there is a statistically significant drop in such crimes which can be correlated to CCTV installation as well as better lighting. ‘CCTV can definitely be said to have reduced overall levels of recorded crime in *only one* system’ (Gill and Spriggs 2005, p. 29 italics added) this finding shows that CCTV is not as effective as is imagined by its supporters. In much the same vein Welsh and Farrington (2008, p. 2) claim that CCTV is useful only for traffic enforcement and reducing crime in car parks. In their study, rates of violent crime were not affected by the usage of CCTV systems. This is interesting for a number of reasons; firstly it would be logical to think that there would be an increase in crime rates at the outset when open air CCTV is installed. This is because if pervasive policing operates according to the logic stated above; then CCTV should at the outset detect a large number of crimes which would affect the overall rate. As these original crimes are detected charged and prosecuted the deterrent effect should take hold as others realise that they are likely to be caught due to CCTV. Thus the original spike in recorded crime should recede according to the received logic espoused by proponents of CCTV. In practice international research has not noted these trends and so the received wisdom and the ‘common sense’ approach to evaluating the efficacy of CCTV must be placed in doubt. One of the foremost reasons for this is that CCTV is effective as a tool against pre-meditated crimes as seen above with the example of property crimes in car parks. Where CCTV is not so useful is as a tool to combat spur of the moment crimes such as assaults, fights or certain types of vandalism such as window smashing which often occur late at night and are linked with alcohol or drug use. Despite this; as we have seen above, it is usually the stated aim of CCTV systems to prevent these types of crime. For example the open air CCTV system in Wexford town was set up with the aim of eradicating late night assaults and as a means of preventing the vandalism of shop windows which was deemed to be a particular problem at the time (Wexford People 19th August 2000).

Despite these questions regarding the utility of CCTV, there is a continuing and steady increase in its use with money being made available in Ireland for ‘community based’ systems. The spread of CCTV can be explained by a number of factors; as outlined

above it is seen as a common sense solution and is often proposed by public actors who wish to appear tough on crime. Past instances where CCTV evidence was useful in identifying and arresting suspects are often mentioned in public discussions. The most famous of these is the footage of two boys leading away the Liverpool toddler Jamie Bulger in the early nineties; and in the contemporary context rarely a week goes by without news reports stating that CCTV footage is being consulted by Gardai investigating a crime. There is also a large security industry in Ireland, suppliers of equipment, maintenance and operatives of these systems will lobby for the use of CCTV to further their financial interests. A further explicative element in the continuing diffusion of CCTV is described by Aaron Doyle who notes the synoptic element which becomes apparent when CCTV footage is used in crime stoppers style programs. In Ireland the longest running of these shows is Crimecall which is run by RTE, the Irish national broadcaster which aims to enlist the watching audience to the role of solving crimes through the use of what Doyle (2006, p. 199) calls 'electronic wanted posters'. Broadcasts of CCTV footage include the audience in the criminal justice process as informers; where they are asked to assist in identifying perpetrators of crime thus categorising criminals as 'others', and creating a mass identity of the vigilant and law abiding viewers.

Recently the commercially run station TV3 has commissioned a number of tabloid style CCTV based shows such as Ireland Caught on Camera. Unlike crime call, these types of shows do not feature appeals for information and instead they aim to shock viewers using CCTV footage. Ireland Caught on Camera claims to 'capture some of the most shocking examples of violence, theft and anti-social behaviour on the streets of Ireland' (found at www.tv3.ie 12-03-2013). The 'realness' of the footage can be sharply juxtaposed with that from television or movies making it 'epistemologically forceful' (Doyle2006, p. 210), and without the gloss of production values CCTV can alter perceptions of crime and violence. As such it is 'important in reinforcing a particular, prominent meaning about crime, one in which for example, crime is portrayed as random, inexplicable violent acts by strangers' (Doyle 2006, p. 200). As well as reinforcing meanings about crime, these shows reinforce meanings about CCTV

surveillance, namely that it is effective and is on the side of the right, honest and law abiding citizenry. If crime is committed by violent others, then CCTV and surveillance systems are on the side of the law abiding who can use them to see justice done and perpetrators caught. In the TV3 show mentioned above an episode entitled 'Drunk and Disorderly' begins with a stern voice over which declares the following.

"every one of us is caught on camera dozens of times a day, as we walk to work, do our shopping, drive back home. Cameras are everywhere and are there to keep us safe, but for those who are up to no good, CCTV is the enemy" (Ireland Caught on Camera, TV3 2012)

The show then continues by displaying footage of street violence interspersed with interview segments from emergency department hospital consultants, victims and CCTV 'experts'. Throughout the program the targets of CCTV are described as 'hoodlums' 'hooligans', 'out of control youths' and 'thugs' who commit acts of 'carnage', 'violence', 'mayhem and destruction'. Those who benefit from CCTV are 'local people' 'in the community' who can 'sleep easy' at night because of CCTV intervention. Interestingly a sizable proportion of the footage displayed is not from CCTV but instead is from mobile phone camera footage which has been posted to video sharing sites such as Youtube; yet this fact is never disclosed. The program also has strong links with the security industry as we are shown a fly on the wall style segment which shows staff from a firm called TEC installing and operating such systems. As well as positioning CCTV as being 'the enemy' of 'those who are up to no good'; a further message from this show is that CCTV is both pervasive and unyielding and as such can be seen as a replacement for the police as an unnamed contributor at the beginning of the program states.

'CCTV can be the police force that never sleeps, it won't look for holidays, it won't go sick, it won't sue you, and all in all it is a boon'(Ireland Caught on Camera, TV3 2012)

Thus the two main messages about CCTV transmitted through this program are that it is on the side of the good and so only those with something to hide should object, and it is a pervasive and unyielding, technologically enhanced means of maintaining order which is more effective than human beings. As well as being more effective, CCTV technologies viewed through this lens are presented as unbiased indiscriminate observers of the urban landscape. The reality however has been shown by Norris and Armstrong (1999, pp. 157-178) to be anything but unbiased as this study which was an institutional ethnography of a CCTV command and control centre showed that 'Male youths, particularly if black or stereotypically associated with the underclass represent the fodder of CCTV systems' (Norris and Armstrong 1999, p. 172). The claims of neutrality afforded to objective technical systems such as CCTV are shown by Norris and Armstrong to be misplaced as the feelings and prejudices of the human operators dictated where the gaze of the cameras were focused. Algorithmic or smart CCTV systems may claim to eradicate operator bias due to the fact they are programmed to spot certain behaviours; yet these systems are still programmed by people and as such are just as likely to have biases and assumptions built into them.

During the interviews the first question relating to CCTV asked respondents if they had ever heard of smart CCTV systems. These systems are attached to computer programs and/or databases which enhance the functionality of the cameras. In Ireland the main smart CCTV system is the Automatic Number Plate Recognition (ANPR) system operated by the Garda Siochana. This system is mounted on speed cameras as well as on Traffic Corps cars and it reads the number plate of each passing motorist while checking the Garda Pulse system database to see if the car is flagged. Cars that are flagged are those which are being used by suspected criminals. The manner in which a car becomes flagged is unclear and does not seem to have much oversight which arguably makes the operation of the system open to abuse. A further element of ANPR is that it cross references passing cars against tax details which means that if the car tax is out of date it will appear on the screen and the Gardai can follow it up.

When asked about smart CCTV systems the majority of respondents had never heard of them, yet when the briefest of descriptions was offered most recognised them and offered numerous examples of their use. Smart CCTV systems have become normalised through their use in seemingly innocuous situations such as car parks or motorway tolling, both were commonly stated examples.

I: have you ever heard of automatic number plate recognition?

R: Oh yeah, Bewley's Hotel, when you drive into it, it spots your number plate, registers it, so they know your car is in eh, your car is in the car park,

I: I'd never heard of that

R: yeah they do yeah, when you drive into Bewley's, I think any of the Bewley's in Dublin, you drive in and there's a camera, and right beside the camera there's a screen and your number plate flashes up and kinda takes the image of the car, so that they know that your car is in the, in there.
(Peter)

I: ok and have you ever heard of automatic number plate recognition

R: no, well I suppose like with the tolls or whatever on the M50,

I: yeah and do ya know anywhere else they're used or any other people who use them

R: em they use them in car parks, like when you're going in it takes a reading of your car reg and then it prints out your location on the ticket like when you go in and get parked
(Hannah)

I:have you ever heard of automatic number plate recognition or ANPR

R: yeah so I guess the toll bridge uses those at the moment

I: yeah and do you know anywhere else they are used

R: eh no, just the toll bridges (Pat)

The use of smart CCTV in a relatively innocuous fashion for seemingly benign purposes such as gathering tolls for motorway use or parking makes these technologies visible to people. This visibility however contextualises these systems in terms of convenience; as being technological fixes which contribute to the smooth running of reasonably complex systems such as motorway traffic or automated car parks. During the interviews there was not one respondent who had considered how such systems could be used to track people's movements and many expressed surprise when this capability became apparent. The most common complaint was that if ANPR does not pick up anything of note then the details should not be kept, as there is no wrong doing there should be no record kept.

R: oh no it's definitely not ok, if you've committed no crime then there's no reason to accuse you or there's no reason or there's no suspicion that you've done anything, I don't think,(pause) that's absolutely totally wrong

I: so you think that if when he passes, if his car tax and everything is up to date that

R: yeah it should be deleted straight away absolutely yeah

(Paul)

In fact however this is not the case, at present every time a car passes an ANPR reader a record of it is kept in the Garda computers. This record is searchable at a later date

which makes it possible for the Gardai to check the historical location of any car that passes a speed camera or traffic corps car. As stated above the Gardai are unwilling to disclose the details of how long this data is kept for and what uses they make of it (See Appendices). In much the same way that CCTV systems are a useful law enforcement tool for after the fact investigations, records gathered by ANPR are also useful in this manner. Their capacity for tracking and monitoring while gathering records was plainly evident when the traffic safety vans were continuously subject to fire bomb attacks at the border between Ireland and Northern Ireland. The reason for the attacks was thought by Police to be that the ANPR systems on these vans were recording smugglers passing by who did not want their movements recorded.

The most common claim made in favour of CCTV is that it creates a feeling of safety, this claim was explicitly tested during the interviews. Firstly respondents were asked 'what do you think about open air CCTV', and the follow up question asked 'does it make you feel any safer'.

I: What do you think about CCTV cameras in public places?

R: I think that they are a necessary evil,

I: Do you feel safer

R: Yeah

I: So say on the main street here at night time, would you feel a bit safer knowing that you're being watched?

R: yeah, I mean essentially it's the same as having all the bouncers which we have now, they're watching us, so if the guards want to watch us as well that's fine. They can catch the bastard who bet up my mate which they did so it's good.

I: so you see cctv as being useful, and since you're not going around kicking people

R: essentially yeah
(Anna)

I: what do you think about CCTV cameras in public places I know we kind of touched on the likes of here like in a hotel or in work but what about even say on the main street?

R: personally I'm all for them I've no problem with them as long as its controlled by supposedly trusted members of the.... as in the Gardai but I wouldn't particularly like it if the cameras were patrolled by say Crimewatch which is a privately owned company. I wouldn't be happy if it was a private company doing it but for the guards then yeah I can see some of the benefits in it, very few cons and a lot of pros.

I: Would they make you feel safer?

R: Yeah, definitely, I think it could act as a deterrent, maybe it's just my age, maybe I'm just getting to that stage where I just want to feel safe and secure these days. I could walk up the main street in a pipe and slippers and say you can't do anything the camera is on me.
(Darren)

In both instances above Anna and Darren are in favour of open air CCTV, Darren sees it as an inherently positive thing, "very few cons and a lot of pros" but his assent to it is predicated on the system being operated by a trusted organisation such as the Gardai. The discourse of deterrence is also evident in Darren's response, yet as we have seen above deterrence is seen only to be effective in crimes which are thought to be planned

or premeditated and so CCTV would be of limited use to deter random violence which happens most often at night and involves the influence of alcohol and/or drugs. Darren explicitly endorses CCTV as a means of increasing feelings of personal safety, "you can't do anything the camera is on me"; so in this case the stated aim of increasing feelings of public safety is met.

While CCTV engenders a feeling of safety with Anna and Darren; this feeling is qualified and subjected to caveats by others.

I: how about, if you gave the example of Henry Street, if Henry Street was kind of bedecked in CCTV cameras would you feel safer because there's cameras all over the place or would you think that it makes a difference to your own personal safety

R: em, (pause) somewhat safer but not totally safe, I think if somebody is completely off their trolley and they're going to attack you, they're gonna do it anyway even if RTE have television cameras beside them I don't think you're going to stop everything like that, again you're going to stop the have a go merchants who are thinking about it and then they realize there's a camera looking at them and they, they have second thoughts on it so yeah I think it does reduce some things
(Pat)

I: here in Wexford town at the minute they have CCTV cameras all over the main street, what do you think of that, do they make you feel any safer or anything like that

R: no I don't feel any safer as a result of them, to be honest with you I never really thought about them, it they don't bother me at all I probably actually have no view on them at all do you know, (laughs) I'm probably not the best person to be interviewing at all like but do you know if they're there it wouldn't really bother me as to whether I'm picked up on them or not you know

I: yeah and do you think they're useful for

R: I'm sure they are useful like for em like the Guards on Friday or Saturday night now I don't know do they ever use the stuff from it or whatever do you know for identifying people or whatever, now there's a friend of ours and he has like a chemist shop down town em and I know on the cctv that they caught people going through his window one time so in that circumstance yes

I: and would you think that people would kind of alter their behaviour if they thought

R: they were being watched all the time

I: yeah

R: if the purpose is to watch people at two o'clock in the morning or whatever then no I don't think they would give a toss do you know 'cos they're full

I: loaded

R: (laughs) exactly yeah I don't know maybe some people would

(Hannah)

Pat sees CCTV as useful as a means of deterring potential assailants yet he does concede that "if somebody is completely off their trolley and they're going to attack you, they're gonna do it anyway" this view is shared by Hannah; "I don't think they would give a toss do you know 'cos they're full". In both of these instances the nature of street violence –ie that it mostly happens at night, and involves alcohol and/or drugs- is claimed to negate the efficacy of CCTV, and so feelings of safety are not ameliorated by it. Anna on the other hand is grudgingly in favour of the systems describing them as a

"necessary evil". She sees them as contributing to her feelings of safety in public and draws on the experience of her friend being assaulted and how in that instance CCTV helped find the assailant, "They can catch the bastard who bet up my mate which they did so it's good". This conception of the use for CCTV is that of its use as an investigatory tool after the fact of a crime which was also mentioned by Paul.

I: and would you feel safer on a street that has CCTV

R: eh yeah I would, I dunno if it's like um if it's an illusion like if you just feel more secure but I would feel a bit more secure like say for talk sake if I was being chased by somebody say along the street I'd probably try and find somewhere where there is a camera just so I could be, you know it's probably fear mongering but you'd hear stories of people being beaten into comas and shit you know, getting the shit kicked out of them, at least if it was on camera or something they'd be more likely to find out who it was so I would yeah, I would feel safer that way em but eh, if they weren't there I probably wouldn't even notice,

The use of CCTV as a tool for investigating crimes after the fact is one of the benefits of systems. While the likelihood of evading an assault is unlikely just because cameras are present, it is the case that some people feel that if they are to undergo such an ordeal; CCTV could help them in the process of bringing the assailant to justice and this can justify open air CCTV on grounds similar to the quote from Marge Simpson at the top of this section. The fear of random and unprovoked violence was a recurring theme in the conversations about CCTV; thus Aaron Doyle could be seen to correct when he links the display of CCTV footage on television to commonly held conceptions about certain types of crime. As well as these examples of responses to CCTV monitoring there were a number of respondents who were in favour of or indifferent to CCTV, yet reported no feelings of an increase in feelings of personal safety.

R:if there's ever any kind of trouble or fights or anything, on the streets em I think that they obviously do, do come in helpful like I mean in the case of an assault or a kidnapping or anything like that they're gonna be very valuable

I: and would you, like say they have cameras around Wexford now, would you feel safer knowing that there's cameras there if you were walking around the street late at night

R: em no, I wouldn't feel safer like, I would feel a little bit more assured that if something did happen to me that there might be a better chance of them catching whoever did it, but it doesn't mean that I'm gonna be walking around thinking that nothing is gonna happen to me just because there's a camera pointed like ……. I mean as far as being like a preventative measure I wouldn't think that they're very useful at all
(Harry)

I: what do you think of video cameras in public places? Like there's a lot in say Wexford Main St now,

R: Yeah no problem, I have no problem with that, at all,

I: Would you think, or even from your own experience would you feel safer say walking down the main street at night because there's cameras there?

R: erm, no, I wouldn't say I'd feel safer, I wouldn't feel any different, but I'd know if anything happens, they're there, now whether they are rigged up to what they are supposed to be rigged up to is a different story but they're there, and if you've nothing to hide, and if you're not going to do anything dodgy then you should have no fear of these things.

I: Ok

R: For example, 2 cars driving down the road, 1 driving perfectly, 1 driving all over the place; you don't notice the guy driving perfectly.
(Peter)

This is a very typical response from the sample when asked about open air CCTV, the majority of those asked claimed to "have no problem" with the systems but by the same token most claimed that such systems did not engender a feeling of safety, with CCTV mostly being seen as being useful after the fact. From Peter's quote above there is an interesting element when he speaks about the two cars. In terms of traffic management Peter rightly points out that the gaze of CCTV will fall on those who don't adhere to the rules of the road. Yet this logic could also arguably be applied to behaviour of pedestrians and people inhabiting urban space where those who are deemed out of place are singled out by the operators and where necessary made the object of police or security intervention. An example of this is found in the store detectives described by Walby (2005) who can identify people who don't belong according to how they are dressed, what kind of bag they're carrying and how they behave. Thus the gaze of CCTV can be said to be normalising; as any people who act differently to those around them are singled out and excluded making CCTV a tool which can be used to carry out 'anthropoemic' (Baumann 2000, p. 101) strategies. Norris and Armstrong (1999) note how CCTV systems are most often operated according to the whims and prejudices of those who occupy the operating room, and this means that young working class males, are most likely to be monitored and followed by CCTV. Thus despite any pretensions to so called smart, or algorithmic CCTV, the systems generally operate as a means of monitoring and excluding a variety of 'others' usually defined as such according to markers of class, race or ethnicity.

If we look once more at the received logic which relates to the efficacy of CCTV it is evident that there is a link to the prevalent metaphor of Panopticism. In a panoptic

enclosure the gaze of authority is constant yet unverifiable; and so the inhabitants of this space must assume that the gaze is constantly on them and behave accordingly. With CCTV if the deterrence effect is to be taken at face value; then it works according to a similar logic as panopticism where the inhabitants adjust their behaviour to suit the norms of the watcher. Yet many open air systems are not in plain sight and cameras are often hidden or at least disguised.

R: yeah because I would have thought if they're there like considering that some of the benefits are that they would kind of put people off crime, putting them off committing crimes so in a way they shouldn't be hiding them, they should be completely visible, there should be a big arrow saying here's CCTV you know a neon arrow pointing towards it or something
(Paul)

This panoptic logic of CCTV is often evident with in-store systems; where a monitor is placed in a prominent position near the entrance to the shop which displays people to themselves as the pass through the doors. In these instances the system makes itself apparent and the message to shoppers that they are being watched is clear. Traffic or safety vans which use the ANPR systems are also brightly marked and parked prominently in view and thus can be said to use their visual presence as a means of changing behaviour. When an approaching motorist sees the van on the horizon he/she slows down thus changing their behaviour. In this sense such cameras are used in a panoptic fashion, where the presence of a watcher or at least the potential presence of a watcher can be said to alter the behaviour of those who are watched. Bogard (1996, p. 25) notes a similar process when cardboard or wooden cut outs of police cars are placed strategically in accident black spots of roads; while this does not happen in Ireland it is the case that any van stopped at the roadside will cause motorists to slow down on the off chance that it is a safety van. With open air CCTV this same dynamic does not work, not all public systems are sign posted, some cameras are disguised as lamps and in the cluttered urban environment they are not always visible. When this happens the so called

deterrent effect must be made null and void as people can't be deterred if they don't realise that they are being watched. Despite this one respondent thought that obscuring CCTV systems made them more effective.

R: they do work em because they were used in that case where a girl was run over on the street by the guy, he came down a one way street and mounted the footpath and hit her, but they do work. With the public they are largely unseen you know the people they forget about them you know, they're not used to being watched so they are largely in the background, I feel uncomfortable when I know that its, it's like somebody sticks a video camera in your face at a wedding you know and you go all quiet you know

(Sean)

The assumption made here is similar to the Hawthorne Effect, if people are monitored and aware of the fact, they will not behave naturally and so obscuring the systems is imperative if they are to be of any use. Unlike the panoptic view of CCTV this sees the systems as almost being like a way of catching people out, by monitoring them without their knowledge. This way of thinking also coincides with the after the fact utility of CCTV,

I: and do you think that somebody is actually watching them or

R: I would say no there's nobody watching them but they're probably recording so that it can be watched so if there is an incident they can be watched and it can be played back like the system we have

This view may be formed by the fact that this respondent has used CCTV in the process of this work as means of managing people from a distance.

The use of CCTV by law enforcement was not uniformly welcomed; an incident which occurred in Waterford city had tainted the view of some people with relation to CCTV.

Here the arrest of a man who was urinating in public was carried out with excessive force, the key element however is that a CCTV operator, Garda John Burke had moved the camera away from the view of the scene on a number of occasions which allowed for the incident to go unrecorded. The Garda in question after a lengthy court case was fired from the force and sentenced to two years in prison for obstructing the course of justice with Judge Leonie Reynolds describing the incident as 'adding a sinister and disturbing dimension' to the assault. This incident was brought up by Margaret who expressed concern at the power of those controlling the systems to contextualise any incident recorded.

I: ok and eh for cctv then what do you think about cameras in public places?

R: I suppose on the streets and that at night time I suppose it's a safety thing that if someone got stabbed or if like I got beaten up I'd like to think that there is a camera em watching that if I couldn't see the person, and then that episode in Waterford with the Guard and that chap getting beaten up, I thought that was terrible that they could immediately turn the camera away I mean they're supposed to be there for your protection I mean I don't know what the guy was doing I don't know besides but I was a bit iffy you know if they are supposed to be there to protect you and the person who is monitoring it should be on your side rather than the guards you know.

The categorisation of cameras as being "there to protect you" is one which as we have seen is common. In this instance however it is the operators of the camera who have the power to control how the footage is interpreted; firstly through pointing the camera away from or towards a particular incident, and secondly through their privileged contextualisation of the images themselves. In this instance a camera was pointed away so excessive force could be used during arrest without there being a record; the absence of a video recording was deemed to be suspect and the Judge found that the diversion was intentional.

The reasons for putting up CCTV cameras in Ireland do not seem to match the actual uses that they are put to. Public discourse among the Gardai, politicians, public figures, and almost any other person or organization in favour of CCTV is that they are useful as a deterrent. Yet many cameras are hidden or partially obscured from view. CCTV has been categorised in the media and broader public discussion as a tool which is aimed at eliminating anti-social behaviour, through cleansing the urban landscape of beggars, drunks and rowdy youth. The anthropoemic strategies of identification and expulsion aim to reimagine urban spaces as uniform, clean, and most of all safe, which makes them suitable as zones of consumption and grants privileged access to those who can afford to partake in consumer society. There was no uniform or distinct view among respondents with respect to CCTV apart from the view that it was a taken for granted aspect of contemporary life.

## 6.6 Conclusion

The data gathered with respect to surveillance and security was quite contradictory. While the discursive repertoire of 'I've got nothing to hide' was prevalent and used as a means of justifying surveillance practices; there was also -often among the same participants- stated resistance to such practices. The sweeping powers of surveillance which gather and store information on everyone were dismissed for a number of reasons including reasons of skepticism as to how well such practices work. The generalised suspicion of such dragnet style surveillance was roundly rejected as being invasive and ineffectual and there was a noticeable cynicism pertaining to the securitisation claims made with regard to terrorism and organised crime. Such claims were characterised in terms of security actors frightening people into surrendering their rights and allowing invasive actions which empowered a number of state, political, and security actors in return for the chimerical and abstract value of security.

As with the previous chapter on surveillance and work, surveillance in terms of security was not simply seen as a top down exercise of power. Surveillance practices, when known about, have facilitated a sense of transparency which can allow for innocence to be proven which again ties in closely with the 'nothing to hide' repertoire. In terms of

policing and security however this is a flawed logic as security actors are rarely transparent and mostly operate in secret for operational reasons, or reasons of security. As well as this two participants noted the trend towards public, technologically facilitated 'policing' of the moral order, particularly through camera phones and video sharing sites. Such practices mean that people who break minor laws that are offensive to the moral code can be subjected to mob style moral opprobrium which can surpass any punishment that can be meted out by the legal system.

# Chapter 7

# Consumerism

‘I shopped with reckless abandon. I shopped for immediate needs and distant contingencies. I shopped for its own sake, looking and touching, inspecting merchandise I had no intention of buying and then buying it. … I began to grow in value and self regard. I filled myself out, found new aspects of myself, and located a person I’d forgotten existed. Brightness settled around me.
(Don Delillo White Noise 1984, p. 84)

## 7.1 Introduction

Consumption has been offered as one of the ordering principles of contemporary Western societies. ‘If there is one agreement between theorists of modernity and those of post-modernity, it is about the centrality of consumption to modern capitalism and contemporary culture’ (Trentman 2004, p. 373). Descriptions of consumption and consumerism usually equate to one of a number of conceptions; the first of which is the hypodermic or magic bullet model of consumers as dupes of the culture industries of advertising and the media. The second is one which describes consumption in terms of acts of self creation which are carried out through the choices of consumers which reflect their own desired self identity. Both of these conceptions of consumerism will be interrogated with close reference to the emerging online economies of social networking, mass customisation and loyalty programs. While surveillance is most often characterised in terms of policing and security; it is in the realm of consumption that many of the most widely used practices have been developed. The argument hereunder will state that contemporary social and technological forms have rendered many of us ‘glass consumers’ (Lace 2005, p. 1) where the scale and scope of data relating to us which is gathered has made us visible to point of translucence.

These social and technological forms also will be examined with reference to Andrejevic (2007) where the technologically enabled blurring of the boundaries between spaces and roles have led to their hybridisation. In this case the hybrid is created by the mixing of

the roles of producer and consumer to create the 'prosumer' (Fuchs 2011). In exploring the online and digital economy, a core set of questions asked as to how much participants knew about the products and services that they used to the extent they had become routine aspects of their daily lives. The aim was to find out how such sites were used and how much participants knew about their operations. The main findings in the area of surveillance of consumption were that there is a distinct lack of understanding amongst the sample with regards to the operation of the information economy. Companies who are using customer information as a profitable resource seem to be doing so without the knowledge of consumers. While many in the sample claimed to be conscious of privacy, the lack of understanding of the information economy meant that there was a distinct variance between described behaviour and actual behaviour.

## 7.2 Consumerism and Consumption

Consumption at the most basic level of definition refers to 'the metabolic cycle of ingesting, digesting and excreting, consumption is … bound by neither time nor history; one of the inseparable elements of biological survival which we, humans, share with all other living organisms' (Baumann 2007, p. 25). There is however a marked difference between consumption and consumerism. Consumerism describes far more than the basic metabolic cycle described above; it describes the social significance attached to the attainment of certain goods products or services. It is an organising principle of many contemporary societies and encompasses the diverse fields of work, identity, culture and economics. The Oxford English Dictionary defines consumerism as 'the preoccupation of society with the acquisition of consumer goods.' (OED) Whereas consumption pertains to the acts of individuals, consumerism is a characteristic of the wider society (Baumann 2007, p. 28). It is also however an individualising force as consumers are 'radically individuated rather than socially embedded' (Barber 2007, p. 36). Consumerism is concerned with the almost ideological links between the attainment of goods and services, and happiness. In the absence of steady, solid foundations on which to build a sense of self identity such as social class or work; self identity has become increasingly anchored around consumer choices. 'Given the intrinsic volatility and unfixity of all or most identities, it is the ability to 'shop around' in the supermarket of

identities … that becomes the royal road to the fulfilment of identity fantasies' (Baumann 2000, p. 83). These choices turn each person from being a 'self-defined person into market defined brand' (Barber 2007, p. 35).

At its simplest level consumerism offers a broad variety, a menu from which identities can be mixed and matched and ultimately chosen; thus people engage in projects of self creation based on a pre-determined list of given choices. People are 'permitted to choose from a menu of options offered by the world but not to improve the menu or the world' (Barber 2007, p. 36). This fact typifies the movement described by Baumann (2007) from societies of production to societies of consumption; or to put it another way, from homo faber to homo consumens. Fromm defines Homo Consumens as the person 'whose main goal is not primarily to own things, but to consume more and more, and thus to compensate for his inner vacuity, passivity, loneliness and anxiety' (Fromm 1984, p. 17). In the movement from societies of production to societies of consumption there has been the concurrent move away from normative regulation and conformity towards limitless desire as 'a society of consumers is one of universal comparison-and the sky is the only limit' (Baumann 2000, p. 76).

The centrality of consumerism to social dynamics has led to the frequent characterisation of contemporary societies as consumer societies. Miller defines a consumer society as 'one in which commodities are increasingly used to express the core values of that society but also become the principal form through which people come to see, recognise and understand these values'(Miller 2012, p. 40). Consumer societies are those in which the economic motor is kept running by the sale and purchase of goods and services, many of which would be characterised as wants rather than needs. The economic health or otherwise of nation states has come to be measured by means of consumer confidence, or animal spirits to borrow a phrase from Keynes. In times of recession, citizens are exhorted to spend; to kick start or stimulate the economy. Just as in times of economic booms, people are warned against 'talking down the economy' or talking the way into a recession. Consumerism is thus a bell-weather for measuring the health of national and international economies. If the collective feeling of economic

health can be maintained; then high consumer spending will result, and money-borrowed or otherwise- will continue to flow through the system. One of the core elements of the consumer society is the substitution of biological needs with created wants. The core aspect of created or superfluous wants is that they cannot –and should not- ever be satisfied. Satiety means calling a halt to further purchasing which as has been shown above has a disastrous consequence for the consumer based economies which are measured as being successful or failing by the level of consumer spending.

Veblen characterized consumption in terms of its ability to display 'pecuniary strength' in differentiating oneself from those who belonged to a perceived lower status position (Veblen 1973, pp. 65-72). Writing at the beginning of the 20th Century he was describing a time of increased physical mobility, in these increasingly mobile societies there was a disassociation from commonly used social cues which aided in placing people into their respective social class positions. 'Conspicuous consumption' (Veblen 1973) therefore acted as a means of displaying belonging to particular social class positions. Baumann (2007, p. 30) claims that Veblen describes the older and different order of the society of producers and so his description of conspicuous consumption differs qualitatively from contemporary understandings. Consumption in the early 20th century was a security strategy, a means of laying claim to higher social position or a means of solidifying ones standing in wider society. Conspicuous or ostentatious goods were a means of displaying wealth, reliability, trustworthiness and so on, and so their function was to bestow these characteristics on the bearer. Such goods also allowed for the synoptic display of status and wealth. The contemporary inflection in the definition of conspicuous consumption is qualitatively different because contemporary consumption is usually characterised in terms of its fleeting and transitory nature where goods or services are consumed on the spot. Veblen was writing of an era where consumer goods 'stood for permanence and continuous reliability' (Baumann 2007, p. 30) which is in sharp contradistinction to the present.

The main characteristic of consumerism is the replacing of needs with wants, it is characterised by the constant fact of changeable desires which can be created,

manipulated, maintained and destroyed by any of the actors in the culture industries of movies television and advertising. Goods aren't conceived of as being built to last, the consumer society has furnished us with the fact of built in obsolescence being a vital cog in the engine which pushes economic cycles along. By way of example; in 2009 the company that makes the plastic clog style footwear known as 'Crocs' found itself in financial trouble despite having sold about a hundred million pairs since 2002. The reason most often given to explain the perilous fiduciary position in which the company found itself in 2009 was not that it had overstretched itself in aggressive over expansion, neither was it was due to greed or malfeasance on the part of the company directors. In fact the company which had sold a hundred million shoes had made the almost terminal mistake of making the shoes well. Where usual consumer products have a built in –or planned- obsolescence period of three to five years; Crocs downfall was that they were too durable and so did not need to be replaced. Because the shoes were durable and the company had reached a sales saturation point there was simply no one left to buy them, and this was why the company ran into financial trouble. The story of crocs could almost be read as a parable of the consumerist economy where products are made *not* to last. In stark opposition; Veblen described ostentatious consumption where products displayed fixity and permanence; contemporary consumer products which are built to these standards pose an existential threat to their manufacturers and so the prevailing consumer norms are towards disposable goods which need to be replaced on a cyclical basis. This fact of planned obsolescence is the foundation on which business cycles are planned and executed and represent many core facets of the consumer economy.

Planned obsolescence takes two main forms; the first is functional obsolescence, and the second is stylistic obsolescence. Functional obsolescence refers to the process whereby a manufactured product has an inbuilt tendency to stop working after a set period of time. So in the example given above of the Croc shoes functional obsolescence of newer models of the shoe may take the form of stitching that will come loose after a set period of time. Functional obsolescence is most obvious in consumer electronics; for example many of the feted products of the Apple Corporation -including but not limited to the iPhone, the iPod or the iPad- have batteries which last for a preset amount of recharges

(Maxwell and Miller 2011, p. 140). The battery in each instance cannot be replaced or repaired by hand so the most common action is to either return the device to Apple for repair –at a cost- or to discard the device and buy a new one. Stylistic obsolescence on the other hand describes the situation where it is not the function of the item which is made redundant, but its style. Most products released are subsequently re-released with the most minor cosmetic changes made to it to justify the title of new and improved. Whether the changes are in size colour or shape, stylistic obsolescence is a means of spuriously updating almost any product, while at the same time rendering its predecessors unfashionable and redundant. Stylistic obsolescence and the tried and trusted ways of packaging and repackaging the same thing in a multitude of ways allows for consumers to personalise and choose the item in a fashion which best represents themselves in a process of identity formation which will be further explored below.

### 7.3 Mass Marketing, Branding and the Persuasion Industries

Consumption can be used to describe the satisfying of *needs* such as the need for nutrition, consumerism refers more broadly to *wants* which are not necessarily essential for survival, and so can to some degree be characterised as trivial. Whereas needs are biologically determined, wants are socially determined and are often artificially created by the panoply of actors in media, advertising and so on who constitute the culture industry. This practice is described by Inglis as being related to a 'global habitus [which] is structured by a discourse which is developed and promoted by corporations through advertising and marketing' (2008, p. 27). The flow of images and discourses which constitute this global habitus is incessant and ubiquitous. In fact in the early stages of the mass broadcast era -of television in particular- the efficacy of media messages in shaping desires and behaviour was often over exaggerated. The so called 'hypodermic' or 'magic bullet' model of the mass media claimed that messages delivered in this fashion could be simply injected into a docile populace who received them at face value without questioning or subverting their content. The operation of these industries has been the subject of acres of print; most famously Vance Packard's 1957 book the Hidden Persuaders, which described the then- nascent practices of social scientists in the employ of the 'persuasion industries' using the 'depth approach' to manipulate an

unwitting populace into spending money. This approach utilised psychoanalysis and symbol manipulation to attach symbolic values and associations with deep seated psychological importance to mundane everyday products. Packard describes how in the mid 1950's these industries were 'systematically feeling out our hidden weaknesses and frailties in the hope that they can more efficiently influence our behaviour' (Packard 1957, p. 12). This influencing of behaviour through subtle manipulation was applied to more than just the sale of consumer products; Packard also describes the beginnings of the now omnipresent industries of spin, branding and packaging of politicians. Edward Bernays wrote in 1928 that:

> 'the conscious and intelligent manipulation of the organised habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power' (Bernays 1928, p. 9).

One of the most common descriptions of the consumer society is that which outlines the power of the media and advertising industries to persuade people to purchase. Central to this schema is the concept of branding, where products and services become more than the sum of their material parts. Branding allows for seemingly asinine products to be imbued with symbolic value, it is this form of value which is granted most importance according to this perspective. Clothing may often be made in any of the global export processing zones (epz) or sweat shops scattered around the developing world; yet a brand adds the real value to such products by 'creating a corporate mythology powerful enough to infuse meaning into these raw objects just by signing its name' (Klein 2000, p. 22). The key element is that it is not the products in themselves that are being consumed; instead it is the constellation of meaning and associations that are attached to them through the process of branding. A brand is a collection of semiotic attributes which act as a means of associating a broad array of meanings with a product. Thus pieces of cotton stitched together by a sweat shop worker in Bangladesh becomes synonymous not with the conditions in which it is made; but instead with the semiotic constellations dreamed up by the marketing departments which are inserted into the collective consciousness via advertising and marketing.

While such breathless accounts of the power of advertising and the broadcast media can still be found; many of the bold claims made by Bernays, and the dire warnings issued by Packard have not come to pass. While advertising budgets for large firms are still measured in the millions if not billions; the efficacy of such advertising is open to question. Firstly the volume of such messages has increased to the level of being a maelstrom, with such an incessant din many –if not most- messages are simply lost in the crowd. As well as this, contemporary anthropological accounts of shopping behaviour such as that undertaken by Miller have claimed that 'the impact of advertising on adult shopping appears on the evidence of my research to be negligible'(Miller 2012, p. 80). The methodology employed by Miller in his study was to follow people – randomly recruited- on their shopping trips. After closely monitoring them during the shopping expedition, he went home with them afterwards and conducted a debriefing interview which aimed to discuss buyer motivations. Price was found to be the most common motivation, with the exhortations of advertising and branding seeming by Miller's reckoning to only apply to children.

### 7.4From Consumption to Prosumption

Half of the money I spend on advertising is wasted but I don't know which half (Wanamaker quoted in Pariser 2011, p. 48 )

Most theories of consumption mentioned thus far are based on what has become an outdated model. Adorno and Horkheimer originally wrote about the culture industry in the 1940's, and Packard wrote the Hidden Persuaders in the 1950's, both of these were written with the 'mass' media being the subject of enquiry. The mass media has not gone away; if anything it has become more powerful; yet it has also undergone qualitative and quantitative changes. The main changes in the operation of the consumer society have been technologically enabled and can be summed up under the broad rubric of the move from mass production to mass customisation. At its most basic level this

change could be described in terms of the application of Taylorist methods to consumption; where rationalisation and segmentation of the market is enabled by ubiquitous data gathering and sophisticated techniques of mining this data. In Taylor's dealings with workers, increases in productivity were gained by gathering comprehensive data on the performance of given tasks. Mass customised models of marketing operate by gathering as much data as possible about the target market and using this data to tailor marketing messages to individuals rather than categories.

> 'In a society in which every realm of life, from the most intimate to the most public, from the exceptional to the mundane, is colonised by consumerism, it is hard to rule out any aspect of the life as not being of interest to marketers.' (Andrejevic 2007, p. 128)

These practices allow for a shift in methods of marketing; from mass marketing where messages are broadcast to a wide audience and therefore will often reach the 'wrong' people, to customised marketing. The best analogy to describe the difference between mass marketing and customised marketing is that which describes the difference between a blunderbuss and a sniper rifle. Marketing carried out through the mass media will usually have some degree of segmentation, -for example male focussed advertisements will be shown during sports events- but generally the message is broadcast to many and so is relatively unfocussed. Customised marketing aims to know the target market and more importantly aims to know where they are, how to reach them, and when in order to maximise sales. The underlying idea of this form of marketing is best summed up by the dictum 'the best predictor of future behaviour is actual past behaviour' (Turrow 2006, p. 291). So by amassing as much data as is available about the past actions of customers, marketers can make inferences about future consumer behaviour and tailor marketing messages accordingly.

Techniques employed in the process of managing consumers to the extent of 'knowing' them have been made easier with the advent of digital technologies but it would be a mistake to link the two. In the early days of mass broadcasting, offers such as free

autographed pictures of radio and television stars were made. To avail of the offer audience members had to send a stamped and self addressed envelope to the show; the aim of these offers was for the producers to gain an idea of the size of their audience for the purposes of pricing their advertising slots. A further method of measuring audience size and penetration levels of marketing messages was used by Archibald Crossley who pioneered the study of household refuse as a means of measuring consumption. 'Crossley's insight was to recognise that the waste stream … could double as a form of information: a by product of consumption that could provide data for the marketing industry' (Andrejevic 2007, p. 86). This idea of consumption generating information about itself and those engaged in it which is in itself a valuable commodity may trace its origins to rooting through rubbish; but nowadays it is one of the cornerstones of information age economies.

In explaining the workings of customised marketing it is useful to employ the concept of 'cybernetic commodities' as described by Vincent Mosco (1996, p. 150). In the act of selling a physical commodity there are a host of meta-data elements which are generated. These data can include what the item purchased is, when, where and/or how it was purchased, as well as any data which can give clues as to the demographic identity of the purchaser. As has been shown above such data is in itself useful to the marketing and advertising industries and as such becomes a commodity itself. By way of example the use of the Amazon website[1] can be considered; if a person goes to the site and orders a book, the commodity is the physical book itself. The cybernetic commodity is the host of data that is generated in the transaction such as the time of purchase, the name and address of the purchaser, the payment method used and the list of other items viewed. The increased value of cybernetic commodities means that in a real sense there is what Andrejevic terms a 'de-differentiation' (2007, p. 107) between consumption and production. If acts of consumption or leisure involve as a by product the production of valuable commodities –ie data- then there is a blurring of the boundaries between acts of consumption and production. This leads to the creation of a hybrid which has been

[1] www.amazon.com

termed the ‘prosumer’ (Tofler 1980) (Pridmore 2012) (Fuchs 2011, 2012) (Ritzer and Jurgenson 2013).

Karl Marx famously stated that the proletariat is ‘a machine for the production of surplus value’ (Cited in Fuchs 2011, p. 297). Prosumption extends the production of surplus value from that which occurs in the workplace to that which occurs in the various sites of leisure. Prosumers ‘are intimately involved in both the design and the production of consumer products’, (Pridmore 2012, p. 323) they generate surplus value in the form of cybernetic commodities described above, but also in terms of content generated online such as music, video, writings and photographs. Thus leisure becomes a commodity generating exercise and so can to some degree be classed as work. In the case of social networking sites and others sites such as Google; the economic model is ‘to accumulate a large number of prosumers that are sold as a commodity to third party advertisers’ (Fuchs 2012, pp. 297-298). Consumer surveillance can be characterised as a form of economic exploitation. Users may get a minor reward such as a discount, or access to a network but once they are inside the ‘digital enclosure’ (Andrejevic 2007, p. 2) every action they take is closely monitored and recorded for the purpose of generating cybernetic commodities. ‘The more an individual wishes to participate fully in the consumer society, and especially in electronic commerce, the more he or she will be subject to deeply intrusive surveillance’ (Lyon 2001, p. 103).

### 7.5 Customer Relationship Marketing

Another term used to describe such practices is Customer Relationship Marketing (CRM), this ‘involves capturing and managing data generated by customers as they select purchase and use products’ (Ball et al 2010, p. 113). Interactivity lends itself well to marketing, digital data generated via the use of a product makes it possible for customers to be ‘remembered’, and this remembering of each customer allows for services and products to be personalised. It is not just the use of a product that generates information; in the online context if a person looks at a product it is enough to gain useful insight. It can thus be claimed that ‘information has become the central economic resource’ (Komito 2004, p. 49) as in the era of mass customisation it is the flexible

production of goods and services which are sold to highly segmented niche markets that are reached via customised marketing.

It is the case then that information has become a massive industry at the same time as it is also generated by mundane and routine activities. This has led to what has been termed datafication. 'To datafy a phenomenon is to put it in a quantified format so it can be tabulated and analysed.' (Mayer-Schonberger and Cukier 2013, p. 78) Datafication involves the transformation of almost any information into a format which is amenable to analysis. Looked at with a suitable level of abstraction social networking sites can be characterised as a means of datafying social interaction. When people communicate via electronic networks a record is kept in a form which makes analysis possible. This makes it possible to undertake processes such as sentiment analysis which can trawl social networks to uncover how people en masse are talking about, or reacting to any particular event. Sentiment analysis is thus very useful for advertisers to find out whether or not their campaigns are working based on how often they are talked about and even by measuring what is said about them. In fact 'analysis of 509 million tweets over two years from 2.4 million people in 84 countries showed that people's moods followed similar daily and weekly patterns across cultures around the world' (Mayer-Schonberger and Cukier 2013, p. 93). The more such incomprehensibly large data sets are gathered and analysed, the more it can become possible for manipulation.

Customised marketing is not only based on past actions, there is also a contextual element to it. If it is known when people are likely to be in any particular kind of mood, it can most likely also be known when they are most receptive to marketing messages and what form these messages should take. Context can be given in terms of mood; if a person posts on a social networking site, their mood can be gauged based on what they post. So if the post makes them out to be sad then feasibly an advertisement offering a product which will cheer them up could follow. Context could just as easily be taken from geographical location. 'The ability to collect users' geo-loco data is becoming extremely valuable. On an individual level, it allows targeted advertising based on where the person is situated or is predicted to go' (Mayer-Schonberger and Cukier 2013, p. 90).

A company with outlets in a city can know when a person who has looked at their content online is in the locality and auto generated advertisements perhaps replete with tailored ‘special offers’ can be sent directly to their phone. Or context could be gathered from the time, if the person wandering around a city is doing so between the hours of twelve and two o’clock on weekday it may well be advertisements for lunch offers that are sent.

## 7.6 Discussion and Results

‘If you’re not paying for something, you’re not the customer; you’re the product being sold’ (Andrew Lewis cited in Pariser 2011, p. 21)

### 7.6.1 The Personal Information Economy

A question asked in the interviews enquired as to whether or not participants would be prepared to give up some of their privacy in exchange for financial reward. This question is one which the research design allowed for comparative analysis as it was asked a number of times under different guises. While the first time of asking was as above, the second and third times of asking occurred after reading some of the content specific vignettes. As well as this participants were asked about some of their consumption habits such as the use of social networking, customer loyalty cards or mobile phone applications. The use of such services revealed the extent to which participants had in practice submitted personal information as part of an exchange and revealed how many were cognisant of the occurrence. The question of giving up privacy in return for financial reward sparked a variety of responses. The most common was to reject the possibility outright:

I: would you be prepared to give up elements of your privacy for financial reward
R: no
I: no
R: no

I: ok that's a straight answer I suppose
R: (laughs) but I'm sure people would, I'm sure people would be eh, because people are motivated by money, but eh I don't, I don't like the idea that they would give you financial reward for invading your privacy, you're into dangerous territory again then, you don't know where it's gonna stop, I mean they might say let us have a look at your text messages as well (Sean)

In this case Sean is reluctant to sell or trade his privacy because he fears the knock on effects of doing so. By trading away some of his privacy Sean fears a normalisation of such practices and fears where the process could end up. This is an example of the slippery slope subject position which states that any measures or practices which are allowed now will be the first in a series. Allowing this one particular measure to happen sets in train a series of other measures which cannot be foreseen and so should be resisted. A further reason for rejecting the proposition of trading privacy for financial reward was that if a person was to do so they would be trading information about themselves; but also about those closest to them.

R: em I, I probably wouldn't be very keen on it, again it probably comes back to how how much value you place on your privacy and you know what you kind of keep to yourself like what you can hold onto, like especially if you're talking about your family and everything else, you wouldn't want to be selling their information, and really by selling your own you're kind of opening them up to it as well (Harry)

Information may well be individualised and nominally refer to one particular person, but by a process of inferences it is possible to use data pertaining to an individual to extrapolate data on the other members of the household. Thus any information given up by any one member of a household can be indicative of the lifestyles of its other members. This is particularly the case with consumer data as for example information relating to food shopping habits of an individual can reveal dietary habits of the household which could in turn be used as part of a pricing mechanism for health insurance.

Another response which was common was that which allowed for some information deemed trivial to be sold, but for strict controls on other forms of privileged information.

I: ok would you ever be prepared to give up elements of your privacy or to give away certain information about yourself for financial reward, so if you were told if you fill out this consumer survey we'll give you vouchers or stuff like that or we'll give you money off your shopping say

R: it depends on the piece if it's a trivial piece of information which is already publicly available possibly, any thing else no not a chance

I: ok and you kind of talk about trivial information, what kind of stuff would you kind of guard the most

R: mm well certainly any financial details that I'd have em anything that can, anything that can be used to possibly clone my identity em be it em certainly my address would be unless the address can be publicly acquired easily enough I wouldn't give my address to anyone, things like age, my date of birth and things like that like eh no private commercial campaign needs that kind of information from a person eh anything to do with details about immediate family members again I don't believe any commercial campaign needs that information (Pat)

I: would you be prepared to give up some of your privacy for financial reward so if you were told if you fill out this form or if you give us this information about yourself we'll give you vouchers or we'll give you

R: it would depend on what the information was, if it's just say my name and my email address or something like that and they want to spam me or whatever then I'd have no bother doing it do you know what I mean

I: mm

R: it would depend on the information

I: and what kind of information, would it be like bank account details

R: no literally no under no circumstances (Hannah)

The differentiation between trivial and important data is essentially predicated on the difference between data which could be used to commit fraud or identity theft and data that couldn't. Privileged data is that which can be used to gain illegal access to bank accounts or to clone a person's identity and borrow in their name. Other forms of privileged data include medical records or anything which could be deemed to cause embarrassment. As has been shown earlier with reference to Solove (2011) and his conception of aggregation this way of thinking is arguably naïve. Aggregation describes how while one piece of innocuous data might be harmless and therefore not valued as private, an amalgamation of a multitude of these innocuous pieces of data can have a mosaic effect of creating a larger and more revealing picture of the person and their behaviour. With this in mind it is conceivable that there is not really such a thing as innocuous or harmless data and it becomes harder to determine what information about oneself should be valued as private. The idea of privileged information is common and usually refers to information which if made public could cause embarrassment or financial loss. The most common sets of information deemed to be private are medical or health information and financial information. In both examples above keeping financial details private is deemed to be of paramount importance.

The privileged status of financial information has obvious causes; with the increase in online commercial activity access to such information can be exceptionally profitable. While it is difficult to accurately assess; Yar (2006, p. 81) quotes figures from American based Internet Crime Complaint Centre (ICCC) which show a 700 per cent increase in reported internet fraud cases between the year 2000 and 2004. With an increase of thirteen percent year on year (Irish Times Thursday May 10 2012) in the numbers of people using online and digital services; it is reasonable to assume that there is a concurrent rise in the number of fraud cases.

In 2008 outspoken newspaper columnist and broadcaster Jeremy Clarkson included his bank account details in his column in the Sun newspaper. He was attempting to play down the importance of a British Government data loss where discs containing the personal details of twenty-five million British citizens went missing. By publishing his

name address and account details Clarkson aimed to demonstrate how there was a public overreaction to the data loss. He later had to admit that a monthly direct debit of five hundred pounds was set up by persons unknown to come from his account, and that he had been mistaken about the consequences of the data leak (BBC News Monday 7 Jan 2008). The move towards online and digitally based commerce has come alongside numerous national and international campaigns to raise awareness of the potential dangers of identity theft and fraud. These campaigns have brought the dangers of online fraud to the fore and have made people more protective of particular types of personal information particularly any information relating to personal finances.

Poster notes how

> "Everyone in the United States now knows about identity theft and probably has some degree of fear and insecurity because of it. People know about it and are anxious about it not necessarily because they have directly experienced identity theft but because the media have relentlessly informed them about it"
> (Quoted in Cole and Pontell 2006, p. 126)

These factors explain the reasons for financial data being privileged. Pat defines trivial information as that "which is already publicly available" yet it is clear from the examples of privileged information that he cites- address, age and date of birth- that he is unaware of the types of information that are publicly available. Most users of social networking sites display an approximation of these pieces of information, as does the voters register which is available for public consultation; as well as this any mail order online services obviously require an address to send the items to.

A number of respondents had no qualms whatsoever with selling personal information for financial reward, the first instance was with Paul who explained the workings of an online market research company which he had dealings with.
I: and what would you think about giving up some of your privacy for financial reward, so, actually you had said to me before about
R: oh the Irish opinions thing

I: yeah, actually explain to me how that works
R: yeah it's em I registered with them it's like a questionnaire, questions about yourself like age, the usual stuff what do you do for a living that kind of thing in general, and they send you surveys to do that fit say someone in my age group, or employment say that kind of category, then they offer I think it's from seventy-five cent up to one fifty for each, depending on the length of it em and they offer like vouchers for Tesco's or amazon but yeah they're usually the kind of tick the box ones, like I did one for Bulmer's like they show you different ads and ask like have you seen this ad and when was the last time you saw it em and did it have an effect on you, this sort of thing em yeah, but none of the information is particularly private it's more a kind of tick the box thing which I don't have anything to hide if they ask me what do you think of Bulmer's or what do you think of this beer, or this tv channel or something like that and stuff that like I wouldn't really have any problem giving that information so em
I: yeah ok, so that is essentially giving up information for financial reward so you think that's ok obviously
R: well within reason yeah, if they were asking say more private stuff, say I would be less likely to do it then (Paul)

The operation of the site in question –www.irishopinions.com- demonstrates the operation of the personal information economy. Users register with the site giving details of their name, address, gender and occupation; as well as this users agree to the installation of cookies on their web browser which will monitor the users' behaviour and actions while they are online. The combination of these pieces of information means that the company can recruit participants for survey and market research projects. By using cookies to monitor online behaviour the company can accurately target very specific groups of people and offer surveys to them. As each survey is completed a minimal credit is made to an account which can be redeemed in the form of vouchers. Interestingly the vouchers themselves are with companies who also use sophisticated data gathering techniques which means that a further iteration of data production is written into the payments given to participants.

As Paul says there is not necessarily any overtly personal information given up and on the face of it he may be right, but at the time of the interview he was unaware of the cookies installed on his browser. While the questions asked in the course of the questionnaires may not be overtly personal, Paul was unaware of the processes by which he was recruited for each survey. The cookies installed on his browser by the marketing company noted the sites he visited, the content he viewed and most importantly for them; the advertisements he looked at or clicked into. This information more so than the information filled in at the registration stage is what determines which surveys or questionnaires he is selected for. The fact that he was unaware of this whole aspect of the process is also quite typical of the personal information economy. It is not the case that the marketing company is pulling a trick; the policies and operations of the company are all clearly on display on their website and they are not doing anything that scores of other companies are not.

The fact is however that most people do not read terms and conditions, and even if they did they are always subject to change without advance notice or notification. A 2008 study found that privacy policies 'are hard to read, read infrequently, and do not support rational decision making' (McDonald and Faith Cranor 2008, p. 6). Amongst the participants of this study only one claimed to read all privacy policies for websites used, with the rest citing reasons similar to McDonald and Faith Cranor for not doing so. In fact the same study calculated the average annual time it would take to read the privacy policies of the numbers of websites visited by the average person. It found it to be somewhere in the range of 81 hours per year at the lower end to skim read, and 304 hours per year at the higher end to read properly. Following on from this they estimated 'that if all American internet users were to annually read the online privacy policies word for word each time they visited a new site, the nation would spend about 54 billion hours reading privacy policies' (McDonald and Faith Cranor 2008, p.18). The McDonald and Faith Cranor study did not take into account the fact that most privacy policies have some form of addendum which make them subject to change at any time without notice. While it is difficult to assess how often such policies actually change, if each of them were to change even once per annum it would involve an exponential

increase in amount of hours spent reading them. These practices are common not just amongst marketing companies but even for the most popular social networking sites and search engines. The usage of online services is most often predicated on user acceptance of policies and terms and conditions set down by the service provider. As has been shown above these policies are generally unwieldy and inaccessible to most users and so are not read. This is clearly evident above in the instance where Paul did not know about the cookies installed by a marketing company on to his web browser despite this information being clearly displayed on the company website.

### 7.6.2 Apps

An aspect of the trade off between privacy and other more tangible benefits which was unforeseen in the research design related to mobile phone applications or apps as they are commonly referred to. Apps are computer programs which are installed onto smart phones; they are generally used to access particular websites. Due to their size; smart phones are not ergonomically suited to typing long web addresses into a tool bar. As well as this using a phone means viewing sites on a smaller screen which means that some websites were unsuitably designed. A solution to these problems is that each website designed an app for using their site on a smart phone. Apps range from newspaper or magazine apps, to games, to betting to education to almost any other use that can be thought of. While many apps must be paid for, there are hundreds of thousands which are given away for free.

Would you be prepared to give up some of your privacy for financial reward, so if you were told em

R: yeah,

I: laughs

R: you don't need to go any further that would be fine with me, I do it day to day, you probably do it day to day that's completely fine with me

I: ok and what about if em even in some of the ways you were talking about that if some of the information is given up and there are ways that you can even do it unwittingly, what would you think if there was some kind of royalty system, you know the way it

works with music, if you write a piece of music then every time it's played you get paid for it, that if they had a way that every time your information was sold on or used that you a portion of that money would go back to you.
R: I suppose there is different levels of it but even at the moment it's kind of, my take on it is that's what you're getting at the moment anyway like for talk sake if you're on your smart phone and you download an app, it gives you a list of what em you know what's that word they use, basically what they're allowed do on your phone if you download this app, basically they can modify and delete your SD card they can globally position you they can read your emails, they can do this they can do that, so you have a choice, there's different levels of privacy, I mean I couldn't give a rats arse if somebody has that as long as I have this app that ....
I: yeah
R: So I am getting paid for it, I'm getting this app by giving up this privacy
I: yeah
R: So already I am getting a kind of royalty
I: so you'd say that it's an element of informed exchange
R: pretty much yeah if you go on to you go on to netflix, I know they are not in Ireland yet but if I go and give the information about the films I like I get a better deal on, by being part of that process I have my downloads or my streams or videos for a cheaper price than I would get down in Xtra Vision so again I'm getting  a bit of a royalty Amazon exactly the same thing, facebook exactly the same thing, I get something out of it, they get a little bit of my information that I know they're not giving me dollars or anything but they are giving me royalties
I: in a service?
R: yeah (Darren)

This is the only response to this question which effectively understood the nature of the personal information economy. The adage from above that if something is for free then you're the product is apt, yet Darren seems to be the only person who understood the nature of this exchange. The first aspect is how he realises that these processes have become knitted into the social fabric, "I do it day to day, you probably do it day to day".

The second and probably most surprising aspect is how little attention is given to the potentially highly invasive functions of some apps "I mean I couldn't give a rats arse if somebody has that as long as I have this app". Darren understands the nature of exchange in the personal information economy; where personal information is swapped for a service and he has no objection to the potential uses for his data. At a later point in the interview he does claim to be selective about which apps he downloads, but this selectivity is based on how useful or desirable the app is and not on how the producers of the app handle his information.

The market for smart phone apps is largely made up of inexpensive or even free apps; as of March 2013 the average app price according to Apple is $1.55 US[2]. Writing in Forbes magazine; Kate Harrison describes the average cost of developing an app; 'a basic content app costs $1000-$4000, a database driven app costs $8000-$50,000, and gaming apps start at $10,000 and climb to $250,000+.' (14 Aug 2012) Due to the fact that many apps are expensive to design and are ultimately sold cheaply or given away for nothing it is necessary for app developers to open up extra revenue streams through the placement of advertisements. A further and more common revenue generator for app developers however is their ability to harvest personal information. In February 2012 a story which was broken by the website venturebeat.com gained prominence across the world media. The story claimed that the harvesting of personal data from phones by apps 'has become an unspoken industry standard' and that 'Facebook, Twitter, Instagram, Foursquare, Foodspotting, Yelp, and Gowalla are among a smattering of iOS application that have been sending the actual names, email addresses and/or phone numbers from your device's internal address book to their servers'(Van Grove Venturebeat 14 02 2012). While many of these companies could justifiably point out that these practices were necessary to provide the product or service in question, public reaction was overwhelmingly negative. Despite this it is arguably the case that the practices seen in the apps market are routine in many online services. Facebook for example is valued in figures of billions of dollars, yet its major asset is information. In most respects

[2] Found at www.148apps.biz/app-store-metrics

Facebook and many social networking sites of its ilk are at their core programs for extracting data about people which can become saleable commodities. In this sense social interaction which is moving online in ever increasing numbers has become subject to ‘datafication’ (Mayer-Schonberger 2013) where it is amenable to capture and commodification.

### 7.6.3The Online Economy of Personal Information

Contrary to conventional wisdom, social networking sites don’t publicise community, they *privatise* it.(Andrejevic 2008, p. 83)

Among the largest organisations in the contemporary online world are the ubiquitous websites of Google and Facebook. Google started out as being a search engine, at the turn of the century it saw off competition from other more established operators such as Alta-Vista, Ask Jeeves and Yahoo among others. The key to the success of the Google search engine has been the quality of its search results which are enabled by the patented page rank algorithm. Moving on from this; Google offered other services such as G-mail which is an email account with unlimited free storage capacity, Google maps which offers interactive digital maps, and street view which gives the capability to look at almost any street in the world. As well as these services Google extended the search engine to include niche searches such as Google scholar which searches academic articles, legal decisions and patents; Google images which searches for pictures, and Google calendar which operates as an address book and scheduling system. As well as these services Google has continued with other innovations such as it’s translate program which claims to be able to translate text between over fifty languages. In 2006 Google paid $1.6billion to acquire the video file sharing site Youtube, and in 2011 it launched a social networking site called Google+. All of these different platforms and programs contribute to what Fuchs (2011, p. 291) calls ‘Google’s empire of economic surveillance’ which has information as its core commodity.

Facebook is currently one of the largest social networking sites (SNS's) in the world. It's current usage statistics in Ireland stand at 48.04% of the general population, and 71.13% of the population who use the internet. (socialbakers.com) Globally Facebook claims to have over 1.06 billion users who log in at least once a month.

> 'Facebook had around one billion users in 2012, who were interconnected through over 100 billion friendships. The resulting social graph represents more than 10 percent of the total world population, datafied and available to one corporation.' (Mayer-Schonberger and Cukier 2013, p. 92)

The popularity of Facebook is not isolated; its predecessors included sites such as Myspace and Bebo, and different regions of the world have other SNS's which are every bit as popular. These include sites such as Orkut –owned by Google- which is hugely popular in the Portuguese speaking parts of the world, or Cyworld which is a South Korean site which is popular across Asia. As well as these SNS's there are other such as Linked in, Academia.edu, Second life and Twitter. These sites are different in certain ways but crucially the same in many others. Second life and Cyworld involve the use of digital avatars and to some degree a simulated digital environment. In both cases the economy of these digital worlds can have counterpoints in the 'real' world, virtual real estate in second life is sold and leased and the virtual currency –Linden Dollars- is convertible to United States Dollars. In fact virtual products such as clothes, hairstyles or cars for avatars, are a market which is ever growing especially since Facebook incorporated games into its operating platform. Twitter involves posting pictures or statements of one hundred and forty characters or less, it is thus most often used as a platform into which links to other articles and sources are posted. Facebook Google+ Orkut and others like it operate in terms of giving the user a virtual space, characterised as being a wall or page. Users can post content such as pictures video or music to their page and others can comment or give signals of approval such as 'liking' on Facebook. The common thread of each of the social networking sites is that they offer users a chance to partake in displays; they allow users to display their preferences in consumption, lifestyle and even political, social, religious and philosophical views. This

culture of display will be looked at in detail in the conclusion chapter but for present purposes it will suffice to note the use of social networking as a form of identity management and maintenance. This is the common thread which links the various forms and manifestations of social networking sites.

A shared characteristic of both Google and Facebook is that many of their products are given for free. There are no subscription charges on either site, and on the face of it the vast range of useful products and services are simply handed over to users who get them without having to pay. Despite this there are regular news reports of valuations of these respective companies which claim them to be worth hundreds of billions of dollars. These facts beg the question as to how exactly such extravagant valuations have come to be accepted; or to phrase the question directly, how do Google and Facebook make money? This question was asked to every participant, all of whom by their own admissions were frequent users of both sites. The fact of the universal usage of both of these sites by all participants forms the main basis as to why Google and Facebook were the precise sites used in the question. The use of Facebook was a recurring factor in the interviews, a number of participants were recruited through it, and among those who were recruited through other means, and arrangements were often made using the site. Facebook usually came up first during discussions on privacy where respondents spoke of its privacy settings. From this point the question as to how the site makes money was asked.

I: So if you say with Facebook there's no subscription charge or anything like that, how do you think they make money?
R: advertising, it would have to be advertising surely,
I: and what about Google as well
R: em that's a good question actually how does google make its money? em I dunno maybe advertising as well but I'm not sure how.
I: ok have you ever thought with Facebook, I mean have you ever seen ads on Facebook?
R: Yeah, not so much any more but yeah,

I: and are the ads, do they usually or ever relate to anything you're interested in?
R: yeah, like some, fuck, some of them are things like make-up, clothes,
(Anna)

While Anna knew that advertising was the main way these sites make money she was uncertain as is evident in her language: "it would have to be advertising surely….. I dunno maybe advertising as well but I'm not sure how". As well as this she had no knowledge of information gathering or personalised advertising and the last sentence of this excerpt should be read as a form of realisation. In the previous sentences leading up to this Anna had been describing how she uses some SNS's and message board forums to get into conversations about consumer items such as make-up and clothes. So when she was asked if the ads she sees ever relate to what she is interested in she realised how the content she placed onto sites was used to focus advertising back to her.

I: yeah ok, how would you think Facebook makes money,
R: (quickly) advertisements.....
I: ok do you ever get kind of focused advertisements like you mentioned there on Amazon if you buy a book next time you go in..
R: I don't really remember but.. what would you call it, I know a friend who picked up on it once but then she'd be doing like multimedia and stuff and she just put something about God in like, oh God in one of her posts and it sort came up like advertising bibles or something to her! (laughs)
(Carol)

The unanimous answer to questions relating to how Facebook makes money was that of advertising and in the example above Carol followed in this trend. Where she expanded on the answer however was in relation to the story from her friend who noticed a correlation between what she posted on her page and the advertisements which were shown to her. This came after she was prompted about focused advertisements in much the same way that it did for Anna; but Carol had recalled a story which she had told before and the idea of focused advertisements was not totally new to her. In this case it

is a rather absurd example: “she just put something about God in like, oh God in one of her posts and it sort came up like advertising bibles or something to her!” It is arguably only because of this fact that she remembered this.

I: and if we go back to Facebook, how do think that it makes money
R: ehm how would it make money, I suppose don’t they have adverts down the side and banners, I would presume that they would sell that advertising space, and that’s how they make money.
I: and what about google, how do you think they make money?
R: em they don’t have ads do they? em I don’t know how they make money now that I think of it

(Margaret)

This exchange is rather typical of the answers given to this question; Facebook has advertisements which appear on the side of the timeline and so are visible. Due to this participants were quick to say that advertising formed the basis of its revenue generation. As well as this; the two examples above illustrate how some people make the connection between the content they positively identify with on Facebook,-through posting, or ‘liking’ or commenting on items- and the advertisements that are shown to them. This connection was made explicitly and without prompting by Paul.

I: if you think of Facebook we’ll start with, how do you think that makes money
R: eh I suppose through advertising, eh, I don’t mind I have the ad blocker thing on mine so it’s handy I don’t get any ads but I know before that I had ads coming up on the right side of the screen
I: yeah
R: yeah and yeah they were always strangely relevant to what I was talking about or what I was posting and stuff
(Paul)

The advertisements which were shown to Paul were "strangely relevant" to the content of his online interactions and this is the key to how Facebook advertising works. In Paul's case he uses adblocker, this is a piece of computer software which blocks any advertisements displayed by the browser. By using adblocker Paul is managing to skip through and be shielded from online advertisements. The use of adblocker is thus characterised by Paul as a means of subverting the economic model of the sites that he uses for free.

R: that's right yeah, all the video ads on four OD it just skips right through them, I'm surprised Facebook haven't copped on to it, I would have thought that because they are losing revenue that they'd be on to it straight away

Once more the sole focus on advertising as the revenue stream of the site is evident; the value generated by users in the process of using the site is unknown to Paul as it is unknown to the majority of other participants.

Google on the other had is rather famously a plain white page with the Google logo, a text box and a couple of buttons. Since there are no visible advertisements it is assumed by many that it does not advertise. This way of thinking was also evident with Sean:
I: and have you ever thought about how Google makes its money
R: no, I haven't but they do have ads on their page, do they even have ads on their page anymore, I don't even know whether they do or not
I: have you ever noticed what kind of ads are there?
R: no I have not, I'm not sure they have ads on there I just have it on the page where there's nothing

As well as this there was a sense of indifference coupled with lack of knowledge:
I: ok, would you use google at all?
R: All the time, that would be my home page.
I: Ok, have you ever thought about how google makes money?
R: No,

I: ok
R: They do their own thing, off with them
I: Have you ever erm, sure even think now what ways do you think a free site like google makes money?
R: advertisements, it has to be advertising and, I don't know actually
I: Ok
R: (laughs) I honestly don't know, I never thought of it
(Peter)

Once again there is the assumption that advertising is the main source of revenue with the exact nature of how it works being unknown. The point here though is that while Peter doesn't know how Google makes money; he doesn't need or want to: "they do their thing, off with them". Services which are offered for free such as Google and Facebook integrate themselves into users lives and this is their main point, yet at the same time many users accept the 'gift' of the service without question. The basis of financial or contractual transactions is that of informed exchange; both parties know exactly what they are gaining and what they are giving up. Yet informed exchange cannot be claimed in the case of free sites where users generate profitable content without knowledge of how it is used or what their 'side of the bargain' is. In this sense it is arguably the case that sites such as Google and Facebook are exploiting the 'labour' of their users.

A further means of advertising which participants mentioned was that of prioritised search results:

I: and how would you think Google makes money
R: eh I suppose is it maybe from selling how high up on the search results you are, say if I typed in Marlboro and there's loads of companies called Marlboro then the Philip Morris company might pay to be put on the top or something
(Paul)

This same process was described by Pat who was knowledgeable in the field due to his work as a computer programmer.

I: and how do you think they make money

R: Google makes money again from, from advertising, again eh I'm trying to think what their sources would be, certainly paid adverts, or sorry paid search terms which are for every search term that you put in, in a shaded, sorry in the results page you'll always get a shaded area with three, three responses that are paid for, and they auction those spaces for key words, they auction those for quite a lot of money, that was their initial revenue stream if I believe em, they would have a lot from em from advertising, they also then would make money from things like em the Google Adwords em and again they've a lot of services on their site which would help companies involved in targeted marketing as well (Pat)

This section describes how Google earns money by selling placement position in search results. One of the first places people look nowadays to find information on almost anything is Google; and this particularly is true with regard to consumer choices. If the first port of call for consumers when they are researching potential purchases is Google; then Google are in a unique position to mediate between those who are selling a product or service and those who are potentially going to buy a product or service. When a search returns its answers on Google there is usually a sponsored 'adwords' results section which prominently displays a number of links belonging to organisations that have paid for the ranking. It is not as simple as the method by which advertisements are paid for and displayed in static media such as in magazines. The Google model claims to use a variety of data related to the search to carry out an auction which decides the relevance of the displayed results. The data used includes the location of the person conducting the search and the actual words used; the aim is to carry out focused advertising or targeted marketing which supposedly eliminates wastage.

R: I suppose the advertising companies aren't just lobbing out ads at everyone willy-nilly they're directing them and focusing them on a specific person

(Darren)

As described above only those to whom the advertisement is relevant will see it as opposed to other types of mass advertising. In the mass marketing model advertisements are broadcast on radio or television or displayed in newspapers or magazines on a one to many basis. The decision of where to place the advertisements will be based on market segmentation; for example during sports events it is primarily male focused advertising, just as during soap operas it is mostly female focused advertising. The mass marketing model however is replete with wastage; the aim of targeted marketing is to eliminate this wastage and to only show advertisements to the relevant people. Adwords thus runs on a cost per click basis; when a person makes a search they are shown links in the adwords section which are relevant to both the searcher and the search. A charge is then levied by Google each time a user is directed to a third party website via the adwords links. This is an example of the mass customisation approach described above (Peppers and Rodgers 1997, p. 12) (Andrejevic 2007, p. 126) which focuses on individuals according to the information gathered about them and customises aspects of the interaction between supplier and consumer. The customised interaction can take the form of varied price structures, or differences in service levels where valuable customers are offered better rates and handled by more efficient staff.

Mass customisation is by no means restricted to Google and Facebook; the means by which information is gathered to cater for the process is central to the operation of the majority of websites. The main means of gathering this information is through cookies; these are small pieces of computer software which are stored in web browsers to track users across multiple sites, remember their preferences and record their online behaviour.

I: how would you think Google makes money
R: eh by selling your information (laughs) and like online advertisements as well like you always see like the sponsored ads like maybe the most popular searches and …. there is kind of obviously there's the thing where if you've looked at a certain thing then maybe like a music site or something like that, or if you're shopping on amazon when

you go back they'll start making suggestions even if you're not logged in like under your account with them that you could be on even with a google search or on other sites where you get pop up ads and they always, they like seem to know number one where you are and then number two kind of things that you might have looked at maybe six months ago, you know they just throw them up there to try and entice you to click on them maybe

(Harry)

Harry understood the operation of Adwords and the nature of mass customisation. When he describes how sites know "number one where you are and then number two … things that you might have looked at maybe six months ago" he comments on it in a matter of fact fashion. He does not refer to this fact in negative terms and instead sees it as a routine part of the online economy.

One participant who voiced an explicit form of unease at these practices was Darren:
I: and do you know how Google makes money?
R: yeah, I shouldn't use them I know because of how much information google track on me because I use Gmail I use the Google plus I use pretty much all the google buttons or their applications I'd use alot of their stuff and yeah I know they have me pretty much sewn up in a bag, they have every bit of history, every bit of information they have,
I: ok, and how do you think they would make money out of that?
R: selling it on, all the adverts that come up on the side of my page, all the adverts that come up on as soon as I click on the internet the add will be directly focused at me depending on what sites I've been on, or any clue words I've given in emails, any thing like that
I: and have you ever noticed something, an add that's been put to you and thought why have they focused that towards me or
R: I've never wondered why I've just gone ah fuck sake there's another bit of my soul gone they've taken another bit off me

(Darren)

While Darren objects to such comprehensive data gathering -"I know I shouldn't use them"- he still avails of a broad variety of Google products and services. This is a good example of what Zimmer refers to as 'the Faustian bargain of technology' (2008, p. 111) where there is something to be given up in the trade between using a service and being used by it. The Faustian metaphor is perhaps given more unwitting credence by Darren when he defines his personal information and identity with reference to his soul: "ah fuck sake there's another bit of my soul gone they've taken another bit off me". In comparison with Peter quoted above "they do their own thing, off with them" this is a type of informed objection, but an objection which does not take the form of action. Even though Darren knows about and objects to data collection; he does not refrain from using the services.

### 7.6.4 Loyalty Cards

'The scheme is driven by this simple piece of plastic, but every time you shop with us we record all there is to know about you': Sarah Baldock Tesco
(quoted in Simm 2007, p. 99)

One of the most common forms of consumer surveillance is one which does not happen online; customer loyalty programs work by attaching each customer to their purchases and making these data available to the company for analysis. The customer must register for the program, giving details which will always include their name address and date of birth and will often include details on family income. Each time the customer makes purchases with the company they present their loyalty card and are given some minor credit or reward. 'In its essence, loyalty marketing is about rewarding those customers who make purchases at a particular establishment'(Pridmore 2010, p. 296). In terms of grocery retailing the first loyalty scheme in Ireland was offered by Superquinn in 1993; although it was not until 2007 that the group started to use the information for data based marketing purposes. Loyalty schemes of a different form are older than this however, for example Texaco offered a points system in the 1980's where purchases gained stamps which could be exchanged for gifts such as golf balls or toys.

This type of scheme differs greatly from the contemporary forms as the data generated by the scheme was not utilised as a resource in the way it is now. The recent turn towards harvesting loyalty scheme data for analysis would not have been feasible before computing power and affordability had reached levels of the mid 1990's. Loyalty cards are increasingly popular; each of the participants in this study used at least one with the Tesco Clubcard being the most popular. This finding of the popularity of the Clubcard is repeated in other sources, 'shoppers use the Clubcard in eight out of every ten trips to Tesco. There are around 25 million in existence, representing 14 million households' (Simms 2007, p. 96).

In the case of the Superquinn Rewards card, the Tesco Clubcard and the Dunnes Valueclub card, each euro spent earns the bearer one point which is ultimately redeemable as one cent. The ratio increases by a multiple of four in Boots, where each euro spent is equivalent to four points and each point redeemable as one cent. The benefits to the consumer are apparent; the more they use the loyalty program, the greater the reward or discount they will earn. The benefits to the company operating the program are on the surface about repeat custom; hence their characterisation as "loyalty" cards. If a customer has been earned through other marketing or advertising practices it costs less to keep them than to seek out new customers. 'A high percentage of a companies profit comes from repeat purchasers … it costs several times more to get a new customer than it does to retain a loyal one' (Turrow 2006, p. 291). By fostering loyalty and repeat custom, retailers are guaranteeing future profitability and are doing so for the minimal cost of one percent of the retail price. The second and more important benefit of loyalty schemes to retailers is that they offer a reasonably inexpensive means of conducting in depth market research. The data generated by loyalty schemes is invaluable to retailers who use 'the consumer information gathered in the programs to create relatively detailed profiles of each consumer' (Pridmore 2010, p. 298). These 'biographies of consumption' (Evans 1998) are valuable commodities and have a number of potential uses; they can be sold to external companies, they can be used in house to tailor marketing campaigns to a highly segmented customer base, and they can

be used to gain efficiency in the supply chain. In the case of Tesco; the operation of the Clubcard loyalty scheme was overseen by the Dunnhunby Group who claim to operate in the field of 'consumer science' which is synonymous with mass customisation as described above.

The prominent use of such data is for panoptic or social sorting (Gandy1993) (Lyon 2007) this involves customer profiling and categorisation where each consumer is placed within assigned market segments so as to offer them differential treatment. This categorisation of people usually takes the form of each person receiving a score which determines the category they are placed in. The most prevalent and wide reaching form of this can be seen in credit scoring; where people are categorised according to their financial history and scored for the purpose of delineating their likelihood of paying back or defaulting on a loan. So in this instance scoring has very real effects on the life chances of people who are often unaware of the criteria by which the scoring takes place. Businesses such as grocery retailers segment their customer base into categories which can range from 'high worth' 'wealthy' and 'frequent' shoppers, to low worth customers often characterised in euphemistic terms such as 'cost conscious'.

> 'Tesco has six broad segments it considers in every management decision-upmarket shoppers, health-focused shoppers, traditional cookers, mainstream families, convenience shoppers and price sensitive shoppers. It also has 17 distinct customer groups which include brand loyals, dieters, calorie loaders, adventurous eaters, promotion-junkies, ethical, green and so on.'
> (Hayward 2009, p. 35)

By attaching these groups of categorised consumers to addresses, it becomes possible to enact a form of geo-demographics. This can take the process of categorisation beyond individual people and bring it to a level of categorisation of neighbourhoods, villages or towns according to their worth to the company. 'The basic rationale behind geodemographics is that "birds of a feather flock together", making neighbourhoods relatively homogeneous' (Evans 1998, p. 57). Thus loyalty card data is instrumental in

making decisions as to where shops will open; areas with high concentrations of low value –or 'cost conscious'- consumers will often find themselves without larger stores. In its most extreme variation this can lead to so called food deserts in low income often urban areas; where an inferred lack of profitability means that larger companies do not set up there. This can lead to a situation where broad varieties of food are unavailable to residents. In the absence of bigger retailer's, smaller shops which are less likely to stock a wider variety of foods are common, as well as this residents of low income areas are less likely to drive and so are unable to use the now common 'edge of town' big box retailers.

The main focus of questioning on loyalty schemes aimed to find out how much was known by participants about them. Older research such as Graeff and Harmon (2002) found that a significant majority of people asked about loyalty cards took them at face value and characterised them in terms of being offered as a means of engendering loyalty and repeat custom. Correspondingly a small minority of those asked had any knowledge or awareness about the use of such cards to gather consumer or marketing data, or of the usage of such data to profile. The fact that this study was undertaken over a decade ago makes it an interesting point of comparison with the present research. It would be expected given the number of data breaches and public attention given to such matters that there would be a difference in knowledge levels between 2002 and 2012, but this was not found to be the case.

During the interviews one of the vignettes told related directly to the operation of retailer loyalty cards. The vignette which was read was:
Mag shops regularly in the same supermarket, she recently accepted a loyalty points card which she presents at the till each time she is shopping. By using the card she gets a discount on her purchases, in return for this the supermarket gets a detailed list of her preferences and they can compile a profile of their customers. The information held by the supermarket is then sold on to other marketing companies. So what do you think of this?

The vignette which is as short and concise as possible aimed to exemplify the operation of loyalty card schemes without bias. The last sentence describes how some loyalty card data can be sold to other sources such as marketing companies. In the interviews the ever present focus of discussion was the Tesco Clubcard as each participant used the service. It is unclear whether or not Tesco sell any information gathered as they refused to disclose this information 'for business security reasons'. (see appendices) They claim that they do not sell any individualised data but do sell data on shopping trends of localised areas allowing for the operation of geo-demographics as described above. It is also worth pointing out however that the 'Tesco Group' does offer services such as financial products, insurance, health insurance life assurance and others which are predicated on gaining knowledge of their customers. As such it may be irrelevant whether a company the size of Tesco sells information or uses it themselves within the broad umbrella of the varied services they offer. Most likely however is that it is a question of semantics when Tesco say that they don't sell personal information just as Google and Facebook say the same thing. While they might not sell actual personal information, they do use personal information to allow third parties to target advertisements, and they charge for this service. Through the operation of the Clubcard and through an aggressive policy of buying up any publicly available data Tesco has expanded its business to become one of the United Kingdom and Irelands largest knowledge brokers.

The most common response to the vignettes on loyalty cards was to accept them at face value and to emphasise how the consumer benefits.

R: No problem with it provided that she knows that the information is used for marketing purposes, that she knows that the details of her shop are tracked and provided that em general statistical details are transferred to the marketing company and nothing that identifies her and what she buys, so say for example like if information like females in the thirty to forty age bracket em buy alot more shampoo than males in the forty to fifty, that type of thing, no problem whatsoever about it, that information once her own personal details aren't transferred yeah I have no problem with that anything outside that yeah, that's not good

I: ok and do you think she is getting a fair deal if she gets her shopping cheaper
R: yeah I think in certain things you get nothing for nothing and eh em but again once it's disclosed beforehand, once there's a proper privacy policy where em on the terms and conditions of the loyalty card that they will not transfer personal information that they will only transfer statistical information for marketing for marketing purposes and you know like one of the benefits of the loyalty card is that she would get discounts on her groceries then yeah I think that's fair enough

(Pat)

This response displays knowledge of statistical uses of consumer data and deems such use of consumer data acceptable as long as it does not pertain directly to individuals. This idea of privacy amongst abundance is relatively common. If information gathered is de-individuated and people are treated in terms of their belonging to a group or category then individual privacy is not harmed. This focus on individual privacy is understandable but does somewhat miss the point. People are categorised more frequently than they will ever realise, and categorisation is by its nature an exercise of power. Categorisation usually is carried out by institutions and the subject of categorisation is usually an individual. When someone is categorised they are shrunk into a form of institutional shorthand which pigeon-holes them to suit the requirements of the institution often irrespective of the needs of the individual. If we use an example of financial institutions; it can be seen that a consumer who is categorised as being low risk and potentially valuable to the institution will pay less for credit. Conversely someone who is classed as high risk will be charged a premium when they apply for credit, thus the people who can actually afford the high rates aren't charged them. 'This emphasis on individual differences leads to two corollary assumptions. One is that marketers should reward their very best customers. The second is that they should push away even alienate those who are less valuable' (Turrow 2006, p. 292).

In terms of categorisation there is also the fact that institutions create the categories that people are placed into and in some ways create the people that are fitted into the categories. This form of institutional interpellation can often operate in terms of a self

fulfilling prophecy; if someone is categorised as being something, they will be treated as such and will eventually in all likelihood begin to act in accordance to the manner to which they are being treated. So if someone is categorised as a credit risk they will be charged a higher premium if they wish to borrow. This higher premium makes it more likely that they will encounter difficulty with repayment, and this in turn makes default more likely making the original label a self fulfilling prophecy. In this sense the labeling that goes on in a consumer context forms a tangible part of what Gandy (2009) terms cumulative disadvantage.

A further response which was common emphasised the convenience which underpins services facilitated by consumer data gathering.

R: well I have a Tesco card and I shop online with Tesco and they keep all my favourites so it's much handier when I go in, everything is there for me so I find that handy, but again I wouldn't like them selling on my details to someone else for their financial gain but I like when it suits me (laughs)

I: do you think there's much occasions  where convenience would outweigh, or do you think they should in no uncertain terms tell you what they do with this information if they

R: I think they should tell you what they do with it but I would hope that they would just use it for the benefit, their benefit of putting my favourites down and making it easier for me to shop but not pass on my details to anybody else but then Tesco now has finance and insurance, and what else do they do pet insurance, they've got a pharmacy in there as well so you wouldn't know once it's in their system where is it going in house as they say.

This section shows once again the balancing act between feelings of apprehension regarding data gathering, and the usefulness of the service offered. With Darrren above this took the form of worrying about the data google have on him and balancing this

worry with the useful apps he gets for free. In this case it is the convenience of online shopping; if groceries are bought online then the weekly shop is stored by the retailer and remembered each time the customer logs in. If the weekly shopping list is stored by the retailer then it is datafied and as we have seen above becomes in itself a commodity. While there are concerns about the sale of such data, these are tempered by the convenience of the service: "I wouldn't like them selling on my details to someone else for their financial gain but I like when it suits me". This response also could be characterised as somewhat naïve; where Pat claims above that "you get nothing for nothing", this response hopes that the data gathered is only used to her benefit. "I would hope that they would just use it for the benefit, their benefit of putting my favourites down and making it easier for me to shop". As has been shown consumer data has become a commodity in itself and as such, instances where it is gathered have become lucrative revenue streams. So in this sense it would be unusual for companies who are routinely gathering such vast data sets to not try to profit from it. What is also interesting is that Margaret is the only person to distinguish between a company that sells data to other companies, and a large organisation that passes data between its own departments: "you wouldn't know once it's in their system where is it going in house as they say".

## 7.7 Conclusion

The movement from the mass production of goods and services to mass customisation and individualisation has happened in concert with the increase in value of cybernetic commodities. We have arguably reached the point where 'flows of information and communication have become more important to the modern economy than flows of physical products' (Van Dijk 2006, p. 70). More interactions –virtual and physical- have become mediated by technology, and these mediated interactions are in themselves productive. The economic model of many of the largest companies is moving towards the gathering of data sets of ever increasing size. In fact a number of these companies such as Google and Facebook are primarily valued according to the data they hold and the potential future uses of it. The services offered by such companies are most often free; but as is evident above it is the use made of these services and the data generated which is of value to them. The key point to be made is that many users do not know how

they are ‘paying’ for the use of these services via their labour as users. In this sense it is an asymmetrical exchange as most users aren’t aware of their side of the deal. Where there is knowledge of consumer surveillance; be it through mobile phone apps, loyalty cards or online services it is usually at best a partial knowledge. Yet even where this is the case, the participants interviewed were usually happy to reap the benefits and convenience of personalised service which is the result of consumer surveillance. There are multiple benefits of individualisation; pricing can be tailored to individuals as opposed to categories, and services can be personalised. Yet these benefits come at the cost of privacy, the comprehensive data gathering which facilitates these processes makes us ‘known’ to institutions in a manner which is unprecedented. In this sense we have become ‘glass consumers’; (Lace 2005, p. 1) this analogy is apt because while glass is transparent it also can distort and exaggerate the image of the object being viewed. Thus profiles or scores which are determined by data are often similar to caricatures; they are determined by a limited aspect of an individual’s character which is over exaggerated. It is thus a one dimensional version of the individual which is the basis upon which life chances can be decided. As well as this; such profiling is a form of imposed identification where recorded characteristics form the basis of how a person is treated and which opportunities are open or closed. In the contemporary age of lasting institutional memory such imposed identities are increasingly difficult to shake off.

# Chapter Eight

# Conclusion and Discussion

## 8.1 Primary Findings

The core findings in this study were that there is a lack of knowledge amongst the sample relating to practices of surveillance and how they operate across the different spheres of social life. As is remarked above in chapter six it is surveillance practices which have been used in high profile instances which are most likely to be known about and acceptable. CCTV was deemed to be the most acceptable form of surveillance and was the most remarked upon. The discourses of safety and deterrence discussed in chapter six pertaining to CCTV seem to have been accepted and internalised. Much of the responses positive to surveillance followed closely with recognisable subject positions such as 'I've got nothing to hide and so have nothing to fear'. As will be discussed in detail below this represents a further internalisation of discourses which benefit large state, commercial, and corporate actors. This subject position is instrumental in the creation of a duality of group identifications; the 'we' who have 'nothing to fear' and so should welcome surveillance, and the 'other'. The other is characterised in terms of being those who have 'something to hide' and therefore something to fear from the institution of surveillance measures.

Surveillance is most typically defined in terms of the operation of a top down mode of power; the participants in this study often made references to instances and practices where this definition could be expanded. Surveillance in these terms was linked to transparency, which could in turn be used to keep more powerful actors -such as the Police or employers- to account. If records are kept on everyone then they can in some instances be used by everyone, whether it is to prove workplace productivity or innocence of a crime. This idea however is fundamentally flawed as records and data which are kept are usually a resource to the organisation maintaining them. This means that there is rarely full and open access, and it is uncommon for such information to be publicly available. During the course of this research two of the largest data holding agencies in Ireland -the Garda Siochana and Tesco Ireland- were approached with

questions relating to the manner in which gathered data is used. In both instances there was a blanket refusal to discuss any aspects of data handling procedure which is evidence of the fact that some actors exercise what is tantamount to a monopoly power over data (see Appendices). As is indicative in these two cases there is an asymmetrical relationship between those who gather information and those on whom information is gathered. This means that in most cases the idea of a holding to account of the powerful via greater transparency is erroneous as those who gather information are usually under no obligation to state how it used. In instances where there is access to data such as in some workplaces where employees have access to performance metrics data and recordings of their telephone interactions, it is possible for such omni-directional surveillance to occur.

There was also a noticeable difference between participants stated positions on privacy and their actions. This became evident during the interviews where people who claimed to be in control of their privacy used platforms and websites which operated in ways that they knew nothing about. Often people who professed to being private, and put much faith in their abilities of managing their online identities partook in behaviour which made such efforts redundant. As well as this there was evidence of a noticeable lack of knowledge in the operation of information capitalism. Whether in the form of how Facebook and Google make money, or how loyalty cards operate, the idea of personal data being a commodity is not one which is commonly held at present. A further aspect of this however is that conceptions of privacy seem to be in flux. Changes in what constitutes the private realm are best exemplified by contemporary modes of entertainment such as reality television and social networking which have normalised the culture of display which will be explored below with reference to Baumann (2011).

### 8.2 Knowledge of Surveillance

The first aim of this research was to ascertain the knowledge levels of participants with respect to practices of surveillance which are sewn into the fabric of contemporary life in Ireland. The results of this were somewhat mixed; while some of the security based aspects of surveillance were relatively well understood by participants, some of the more

routine practices were not. So while some knew that using a mobile telephone allowed for the system to record the movements of users, very few knew anything beyond a cursory understanding of how Google or Facebook operated. The reason for this, which became clear throughout the conversations, was that security based surveillance which would be used in prosecuting criminals is most likely to be reported on in the media. With such methods of surveillance occasionally being the subject of public discussion, it was more likely that participants would know about them. In the case of mobile phone surveillance, it was the prosecution of Joe O'Reilly for the murder of his wife (see chapter six) which seemed to trigger the association amongst participants. The instance of knowing or not knowing about surveillance practices in this study had no correspondence with either age or socioeconomic status. As this study utilised a small sample, such patterns were not evident, yet further research using a larger sample could reveal the presence or absence of such patterns.

### 8.3Surveillance Practices in Consumption and Online

Each interview began with a list of surveillance technologies and practices being read aloud, and participants being asked if they had ever heard of them. The overwhelming trend was that very little was known about many surveillance technologies or practices. As well as this, during conversations with participants it became clear that little was known about the potential consequences of pervasive surveillance. These findings point to the necessity for some form of public education and/or discussion regarding surveillance. In particular there is a need for public discussion on the use of search engines and social networking sites and the potential uses made of data which is freely surrendered by users. There are many benefits to surrendering such information, social networking sites are fun and useful for maintaining friendships, particularly weak ties. Such sites are essential for networking and are useful for gaining and maintaining weak tie friendships which are important as they allow people to 'get ahead rather than get along' (Rice 2013, p. 177). In an era of weakening security around employment and an increase in short term and casualised labour, such networks of loose associations could prove essential for gaining employment. Yet the negative aspects of such sites are that they leave behind a permanent trace of all interactions, photographs, conversations, and

even locations of users. As has been shown these records are a valuable commodity for which the 'payment' is use of the site. Services which are offered for free such as Google and Facebook integrate themselves into users lives and this is their main point, yet at the same time many users accept the 'gift' of the service without question. The basis of financial or contractual transactions is that of informed exchange; both parties know exactly what they are gaining and what they are giving up. Yet informed exchange cannot be claimed in the case of free sites where users generate profitable content without knowledge of how it is used or what their 'side of the bargain' is. In this sense it is arguably the case that sites such as Google and Facebook are exploiting the 'labour' of their users.

Where it was the case that participants claimed to be in the know about managing their data, and being in control of their digital identity; it was usually also the case that there were significant lacunae in their knowledge. One participant who was registered on a social survey site did not know that the company he was registered with was monitoring his online activities via cookies. In fact when asked, only three participants could give an adequate explanation as to what cookies are or what they do and one of these participants was a computer programmer. A further point of note is that amongst those who claimed to be in control of their online identities were people who claimed to read privacy policies and the terms and conditions of websites. Whether or not this is the case, the fact is that 'most companies reserve the right to change the rules of the game at any time' (Pariser 2011, p. 239). This means that even if a miniscule number of people take the time and effort to read the densely written, jargon filled legalese which constitutes most privacy policies they are subject to retrospective change at any time without any legal requirement for user notification. This in effect makes it difficult if not impossible for the effective management of online identities.

### 8.3.1 Cultures of Display

In the course of the interviews, a common thread was the use of social networking. In a number of cases, interviewees spoke in terms of their pages being not just a means of communicating with friends but a means of broadcasting. Patrick explained how he used his Facebook page as a means of telling jokes which he posted everyday in his status

updates. These jokes were often ridiculous retellings or parodies of current events into which he put a lot of time and effort, actively courting an audience. Sean is active in Irish politics, and when he was asked how he uses privacy settings on social networking sites he said:

> R: Most of what I say is for public consumption, I don't use my facebook to keep in touch with my family, or friends either, I have a lot of my friends that are on it but anything that's on it is of a political nature and is generally for public consumption and I want people to see it, I use facebook as a propaganda tool for my work you know, it's not eh even though I set it to private there's over a thousand people who are on it most of whom I wouldn't know. (Sean)

These two instances show social networking not as being a method of two way communication like a telephone, but instead being a means of broadcasting, a means of display which allows users to claim particular identities such as in these two cases the humorist and the social commentator. Other respondents noted that they used social networking to display cultural or consumptive preferences in order to bond with others of similar interests, in what Castells refers to as 'networked individualism' (2001, p. 129). Using the internet and particularly social networking sites as material supports for networked individualism, respondents build what Castells calls 'portfolios of sociability' (2001, p. 132) where multiple but weaker ties are created and maintained, centered around choices of lifestyle, consumer, or cultural preferences. These ties often correlate to offline networks - online communication and sociability is matched in the 'real' world. Yet there was significant mention of sociability in the 'space of flows' (Castells 1996, p. 408) where communication is global, technologically mediated and spatial differences are compressed to nothing. Peter, 45 year old and heavy user of the internet in this manner states:

> R: We live more separately, but we don't, you know, we live more separately to our next door neighbour, but we live closer to the guy across the world. (Peter)

The usage of electronically mediated communication raises interesting questions regarding the nature of contemporary community. It is not just the case that we use globally interconnected digital networks to communicate free of the constraints of geographical location, with people from all over the world. The evidence of this research is that it is predominantly locally based peer groups who use technologically mediated means of communicating, even when there is no significant geographical divide. As has been shown above; such means of communication leave behind records which are valuable commodities. Local communities thus become monitored and mediated by numerous third parties such as social networking sites as they go about the routine process of communicating amongst themselves. Conversations which once would have taken place over the garden fence now occur across digital networks, which make them amenable to capture, as a valuable resource. This 'datafication' (Meyer-Schonberger 2013, p. 73) of social interaction commodifies it, and repositions sociality as a resource. As has been shown in the preceding chapters these resources are useful to a broad spectrum of actors including those of business, finance, marketing, security and policing to name but a few. At the same time however; this research contends that users are not sufficiently knowledgeable about their data trails, and in general do not realise the manner in which their data is used.

One of the more striking findings of this study is the changing nature of privacy which is best illustrated by Baumann:

> 'In our days it is not so much the possibility of betrayal or violation of privacy that frightens us but in fact it's the opposite: shutting down the exits from the private world, turning the private domain into a site of incarceration, a solitary confinement cell' (Baumann 2010, p. 31).

Baumann (2010, 2011, 2013) characterises privacy as having changed, from being a valued inviolable space within which personal development and thought can occur free from the eyes of the world, to being a prison which prevents people from being seen or

being on display. This change could be seen as a reversion of meaning to the Latin etymological roots of the word 'privare' which meant to deprive 'as the connotation for classical thinkers was very much to do with deprivation rather than voluntary withdrawal' (O'Hara and Shadbolt 2008, p. 21). Privacy in this sense was the domestic realm where very little happened, as opposed to the public realm of the polis where all governance, trade, commerce and public discussion occurred. Networked communication in general, and social networking sites in particular, bring the outside world of the polis directly into the domestic realm, blurring the boundaries between the two. In another article Baumann rewrites Descartes proof of existing 'I think therefore I am, to 'I am seen therefore I am' (2010, p. 20).

As shown above, users of social media often see it as a means of more that just a means of direct communication; it is used as a means of presentation management, where identities are constructed, presented and maintained. The assertion of such identities is carried out through online displays, and their validation occurs through interaction or feedback from viewers. This culture of display has been synoptically normalised through the mass media in general and reality television in particular. This synoptic normalisation has had the dual effect of increasing the social desirability of being on display via social networking sites, and of minimising apprehensions around the loss of privacy and concerns over surveillance. The social desirability of being on display is further compounded by a common feeling that surveillance measures are aimed at those who have 'something to hide' and so by extension transparency is aligned with the law abiding. To resist or dissent against surveillance, and to stake a wider claim for privacy has negative connotations. These two parallel processes can partially explain the seeming paradox between notions of privacy and the prevailing trends of networked communication, consumption and work. Moreover, these processes coupled with a low level of knowledge, serve to explain exactly why there is seemingly a general indifference towards surveillance and the ever increasing colonisation of the private sphere by digital enterprises.

## 8.4 State Securitisation Practices

### 8.4.1 Nothing to Hide?

A recurring rebuttal to questions asked about surveillance is some variation of 'I've nothing to hide and therefore nothing to fear'. This rationale recurs across many strands of international research into surveillance (O'Hara & Shadbolt, 2008; Schneier, 2008; Solove, 2011). Schneier claims that this phrase is inaccurate because it fails to adequately account for a full definition of privacy, and sees it just as being about 'hiding a wrong' (2008, p. 79). Privacy in these terms is seen as a screen behind which illegal or immoral deeds can be obscured. As has been shown above (Chapter three) privacy is much more nuanced and complicated and is irreducible to such narrow conceptualisation. Privacy is a socially constant yet culturally determined value; almost all cultures have some degree of privacy relating to the body which can differ significantly according to cultural or religious values. Nissenbaum (2010) and Zimmer (2008) describe privacy in terms of contextual integrity which claims that information is never reducible to a simple either/or public or private schema which is universally applicable. There are implicit and explicit norms associated with almost every social situation which "explain the boundaries of our underlying entitlements regarding personal information, […] our privacy is invaded when these informational norms are contravened" (Zimmer, 2008, p. 115). Thus instead of keeping to a simplistic dyad of public/private, contextual integrity looks to the social context in which the information is requested and looks to see whether the request is appropriate for the situation.

Solove (2011) makes three points of reference in response to the "nothing to hide" argument: these are aggregation, exclusion and distortion. Aggregation describes how while one piece of innocuous data might be harmless and therefore not valued as private, an amalgamation of a multitude of these innocuous pieces of data can have a mosaic effect of creating a larger and more revealing picture of the person and their behaviour. With this in mind, it is conceivable that there is not really such a thing as innocuous or

harmless data and it becomes harder to determine what information about oneself should be valued as private. Exclusion describes when the data controller excludes the data subject from accessing or challenging any data held about them. Distortion refers more generally to the images created in a mosaic fashion through aggregation of data and how such images will never be fully accurate and will only describe the elements of a personality that happen to be amenable to capture by these methods. These pieces of data are rarely contextualised and give a bald, one dimensional version of selfhood which is rarely accurate.

Aside from these concerns is the simpler questioning of institutions themselves. While institutions or organisations may be trustworthy and have strict data handling procedures, the institutions are comprised of people who may be dishonest, curious, unmotivated, corrupt or even simply inept. It is best summarised by O'Hara and Stevens who said in response to the 'nothing to hide nothing to fear' argument:

> "if you keep within the law, and the government keeps within the law, and Its employees keep within the law, and the computer holding the database doesn't screw up, and the system is designed according to well-understood software engineering principles and maintained properly, […] and all the data are entered carefully, and the police are adequately trained to use the system, and the system isn't hacked into, [… then] you have nothing to fear" (O'Hara and Stevens 2006, pp. 251-252).

The view that only people with something to hide should value privacy is one which is overly simplistic. As we have seen it is almost impossible to know which information should be classed as private without having it contextualised; in the days of pervasive data gathering, the mosaic effect as described by Solove (2011) shows how any piece of information can be potentially sensitive when it is combined with others. Moreover, for the reasons outlined above by O'Hara and Shadbolt (2008), institutions cannot always be trusted as they can be prone to leaking information. These facts render commonly held

ideas about surveillance and privacy problematic; therefore, there is a need to explore the manner in which these concepts are understood and valued.

The phrase ‘I’ve nothing to hide’ recurred across the interviews with such frequency as to warrant calling it a default position. This common retort has been used to counter arguments against a number of surveillance technologies, from identity cards and CCTV systems to DNA databases among a multitude of others. This view –which is arguably approaching the statues of hegemony – clearly benefits those who have the most to gain from surveillance, such as the large bureaucracies of the state and the private sector. The hegemony of a view which benefits powerful interests raises interesting questions: how has such widespread diffusion of this view been achieved? How has this view been inculcated and internalised by so many people? Both of these questions are important enough to warrant further research.

### 8.4.2 Surveillance and the ‘Other’

The ‘nothing to hide’ view creates a dualism in common consciousness between ‘us’ who obey the law and thus have ‘nothing to fear’, and ‘them’, drawn from the class of the criminal ‘other’ who stand to lose from whatever surveillance measure is in question. By creating such a positive collective identity, proponents of surveillance assure its social desirability and thus mass adherence. Furthermore, this belief inoculates proponents of surveillance against any discussion about the necessity or validity of any surveillance measure. When surveillance is characterised as targeting only those with something to hide, by extension the same characterisation is applied to those who reject surveillance measures. Thus there are positive associations with compliance, and negative associations with resistance. By creating a group of ‘others’ ‘a dominant group defines into existence an inferior group’ (Altheide 2003, p. 18) which can be the focus of criminal sanctions, public fears and the securitarian gaze of surveillance. Garland has theorised the criminology of the other which is ‘a politicised discourse of the collective unconscious’ which ‘relies on an archaic criminology of the criminal type… who typically belong to racial and cultural groups bearing little resemblance to ‘us’’ (Garland 2001, p. 135). So the targeting of surveillance at the ‘other’ refines the membership of

the dominant group, who in this case underline their membership through their tacit or explicit assent to surveillance measures. If surveillance is focused only on the other, then it acts for the protection of the dominant group, thus only those who are outside the dominant group –ie those who don't obey the law- need to worry about surveillance.

## 8.5 Conclusion

As more routine aspects of life are becoming technologically mediated; there are questions raised about levels of surveillance built into the networks which are privately owned, for profit enterprises. These virtual, mediated public spaces make a permanent record of interactions, consumer preferences, political beliefs and opinions. These records are valuable commodities that are packaged and sold across the global marketplace, or surrendered to Police and Security services upon request. Thus it can be claimed that this process commodifies social interaction; which is becoming more routine with the ever increasing popularity of electronically mediated communication. While there is an elementary level of knowledge regarding the potential for surveillance and the threats to privacy built in to contemporary technologies; this knowledge is tempered by the broader cultural processes mentioned above which have normalised practices of transparency and display.

## References


Agamben, G. (2005) *State of Exception.* Chicago: University of Chicago Press

Ahern, D. (2009) *Enactment of the Criminal Justice (Surveillance) Act 2009.* Irish Times 14-07-2009

Allen, A. (1988) *Uneasy Access: Privacy for Women in a Free Society.* Rowman and Littlefield

Altheide, D.L (2006) *Terrorism and the Politics of Fear.* Rowan Altamira

Altheide, D.L (2003) *Mass Media, Crime and the Discourses of Fear.* The Hedgehog Review Fall 2003

Altheide, D.L (2002) *Creating Fear: News and the Construction of Crisis*. Transaction Publishers

Altman, I. (1975) *The Environment and Social Behaviour: privacy, personal space, territory, crowding.* Monteray, CA: Brooks/Cole.

Amárach Research. (2011) *The Smart Future: An Amárach Briefing May 2011*. Retrieved from http://www.amarach.com/assets/files/The%20Smart%20Future.pdf

Andrejevic, M. (2008) 'Mining the Wealth of Online Communities' *Soundings: A Journal of Politics and Culture* 39 (12): 75-87

Andrejevic M. (2007) *iSpy Surveillance and Power in the Interactive Era.* University Press of Kansas

Andrejevic, M. (2005) *Reality TV The Work of Being Watched.* Rowan and Littlefield Publishers

Andrejevic, M. (2002) 'The Work of Watching One Another: Lateral Surveillance, Risk and Governance'. *Surveillance and Society*, 2 (4): 479-497

Ball, K. S. (2010) 'Workplace Surveillance An Overview'. *Labor History*, 51 (1): 87-106 Routledge

Ball, K. S. (2001) 'Situating Workplace Surveillance: Ethics and Computer Based Performance Monitoring'. *Ethics and Information Technology,* 3 (3) 209-221

Ball K. S. Daniel, E. Dibb, S. Meadows, M. (2010) 'Democracy, Surveillance and "knowing what's good for you": the private sector origins of profiling and the birth of "Citizen Relationship Management"'. In: Haggerty, K.D. and Samatas, M. (2010) (eds) *Surveillance and Democracy* Routledge

Ball, K.S. and Wilson D. (2000) 'Power, Control and Computer Based Performance Monitoring: A Subjectivist Approach to Repertoires and Resistance'. *Organisation Studies* 21 (3):539-565

Barber, B.R. (2007) *Consumed How Markets Corrupt Children, Infantalize Adults, and Swallow Citizens Whole.* Norton, New York

Barry, J. (2010) 'The Criminal Justice (Surveillance) Act 2009: An Examination of the Compatibility of the New Act With Article 8 of the European Convention on Human Rights' found at www.corkonlinelawreview.com accessed on 14/02/2013

Barter, C., & Renold, E. (1999). 'The Use of Vignettes in Qualitative Research'. *Social Research Update, 25*(2):1-7. Retrieved from http://sru.soc.surrey.ac.uk/SRU25.html

Baudrillard, J. (1983) *Simulations.* Semiotexte

Baumann, Z. and Lyon, D. (2013) *Liquid Surveillance.* Polity

Baumann, Z. (2011) *Collateral Damage: Social Inequalities in a Global Age.* Polity

Baumann, Z. (2010) 'As the Birds Do'. In: Baumann, Z. *44 Letters from the Liquid Modern World.* Cambridge, Polity

Bauman, Z. (2010) 'Strange Adventures of Privacy (2)'. In Baumann, Z. *44 Letters from the Liquid Modern World.* Cambridge, Polity

Baumann, Z. (2007) 'Collateral Casualties of Consumerism'. *Journal of Consumer Culture* 1(7):25-56

Baumann, Z. (2007) *Consuming Life.* Polity Press

Baumann, Z. (2006) *Liquid Fear.* Polity Press

Baumann, Z. (2005) *Work, Consumerism and the New Poor.* Open University Press

Baumann, Z. (2000) *Liquid Modernity.* Polity Press

Baumann, Z. (1998) *Globalization: The Human Consequences*. Cambridge Polity

Beck, U. (2002) 'The Terrorist Threat World Risk Society Revisited'. *Theory Culture and Society*. 19(4):39-55 London Sage

Beck, U. (1986) *Risk Society: Towards a New Modernity.* London Sage

Bell,G. and Gemmell, J.(2010) *Your Life, Uploaded: The Digital Way to Better Memory, Health and Productivity.* New York Penguin

Bentham, J. (1791) *Panopticon or Inspection House Volume 1*. Google Books

Bentham, J. (1995) *The Panopticon Writings* Ed. Miran Bozovic, London Verso

Bernays, E. L. (1928) *Propoganda* Ig Publishing

Bogard, W. (2006) 'Welcome to the Society of Control: The Simulation of Surveillance Revisited'. In: Haggerty, K.D. and Ericson, R.V. eds. *The New Politics of Surveillance and Visibility.* University of Toronto Press

Bogard, W. (1996) *The Simulation of Surveillance Hypercontrol in Telematic Societies.* Cambridge University Press

Bradley, J. (2008) *Cadbury's Purple Reign: The Story Behind Chocolate's Best Loved Brand.* Wiley

Braverman, H. (1974) *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century.* Monthly Review Press

Brodeur, J. (2007) 'High and Low Policing in Post 9/11 Times'. *Policing: A Journal of Policy and Practice* 1(1) 25-37 Oxford

Brodeur, J. (1983) 'High Policing and Low Policing: Remarks about the Policing of Political Activities'. *Social Problems* 30(5): 507-20

Brodeur, J. and Leman-Langlois, S. (2006) 'Surveillance Fiction or Higher Policing?'. In: Haggerty K.D. and Ericson, R.V eds. *The New Politics of Surveillance and Visibility.* Toronto.University of Toronto Press

Brooks, L. (2007) 'CCTV is No Silver Bullet- It Risks Making Life Less Safe', *The Guardian,* 1 Nov. Available from www.guardian.co.uk/commentisfree/2007/nov/01/comment.politics accessed 24/01/2013

Bryman, A. (2008). *Social Research Methods* (4th ed.). Oxford: Oxford University Press.

Buzan, B. (1983) *People, States and Fear: The National Security Problem in International Relations.* Wheatsheaf Books

Byrne, B (1998) 'Qualitative Interviewing'. In: Seale, C. (ed) *Researching Society and Culture.* London Sage

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

Castells, M. (1996) *The Information Age: Economy, Society, and Culture Volume 1 The Rise of the Network Society.* Sussex, Wiley-Blackwell

Central Statistics Office (2011) *Information Society and Telecommunications in Households 2009- 2011* retrieved from www.cso.ie/en/media/csoie/releasespublications/documents/informationtech/2011/isth2009-2011.pdf

Clarke, S. (1990) *New Utopias for Old: Fordist Dreams and Post-Fordist Fantasies.* University of Warwick

Clarke, S. (1990) *The Crisis of Fordism and the Crisis of Capitalism.* University of Warwick

Clarke, R (1988) 'Information Technology and Dataveillance'. In: Dunlop, C. & Kling, R. (eds) *Controversies in Computing* (1991) Academic Press

Cohen, S. (1972) *Folk Devils and Moral Panics: The Creation of the Mods and Rockers.* Routledge

Cole, S.A. and Pontell, H.N. (2006) '"Don't Be Low Hanging Fruit": Identity Theft as Moral Panic'. In: Morahan, T. (ed) *Surveillance and Security Technological Politics and Power in Everyday Life.* Routledge

Coleman, R. and McCahill, M. (2011) *Surveillance and Crime Key Approaches To Criminology.* London Sage

Coleman R. and Sim, J. (2000) ''You'll Never Walk Alone': CCTV Surveillance, Order and Neoliberal Rule in Liverpool City Centre'. *British Journal of Sociology*, 51(4):623-639

Coleman, R. (2004) 'Reclaiming the Streets: Closed Circuit Television, Neoliberalism and the Mystification of Social Divisions in Liverpool UK'. *Surveillance and Society.* 2(3):293-309

Comscore (2011) *The 2010 Digital Year in Review* retrieved from www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_Europe_Digital_Year_in_Review

Cusack, J. (2012) Gardai dismiss newest 'apparitions' of Murphy *Irish Independent* 15/04/2012

Delillo, D. (1984) *White Noise.* Picador ,New York

DePaulo, B.M. Lindsay J.L. Malone B.E. (2003) 'Cues to Deception'. *Psychological Bulletin* 129(1):74-118

DePaulo, B.M. Wetzel, C. Sternglanz, R.W. Walker Wilson, M.J. (2003) 'Verbal and Nonverbal Dynamics of Privacy, Secrecy, and Deceit'. *Journal of Social Issues*,59 (2):391-410

Doyle, A. (2006) 'An Alternative Current in Surveillance and Control: Broadcasting of Surveillance Footage of Crimes'. In: Haggerty, K.D. and Ericson, R.V. (eds) *The New Politics of Surveillance and Visibility.* Toronto. University of Toronto Press

Elias, N (1994) *The Civilising Process.* Oxford, Basil Blackwell [1939]

Emmers, R. (2007) 'Securitization' in Collins (ed) (2007) *Contemporary Security Studies.* Oxford University Press

Ericson, R & Haggerty, K. (1997) *Policing the Risk Society.* Toronto. University of Toronto Press

Etzioni, A (1999) *The Limits of Privacy.* Basic Books

Evans, M. (1998) 'From 1086 and 1984: direct marketing into the millennium'. *Marketing Intelligence and Planning* 16 (1):56-67

Finch, J. (1987) 'The Vignette Technique in Survey Research'. *Sociology*, *21*(1):105-114

Foucault, M. (1978-79) *The Birth of Biopolitics Lectures at the College De France.* Palgrave McMillan

Foucault, M. (1977) *Discipline & Punish: The Birth of the Prison.* (2nd ed.). Knopf

Doubleday Publishing Group.

Foucault, M.(1972) *The Archaeology of Knowledge.* London Routledge

Fraser, M. (2011) 'Viral Vigilantes: The Unblinking Panopticon and the Wheelie Bin Cat Lady'. Paper Presented at *Cyber-Surveillance in Everyday Life: An International Workshop* * May 12-15, 2011 * University of Toronto

Fromm, E. (1984) *On Disobedience and Other Essays.* Routledge

Fuchs, C. (2012) 'Critique of the Political Economy of Web 2.0 Surveillance'. In: Fuchs, C. Kees, B. Albrechtslund, A and Sandoval, M. (eds) *Internet and Surveillance The Challenges of Web 2.0 and Social Media.* Routledge

Fuchs, C. (2011) *'Web 2.0, Prosumption and Surveillance'. Surveillance and Society* 8(3):288- 309

Fuchs, C. (2011) How Can Surveillance Be Defined? *Social Networking Sites in the Surveillance Society*, 5(1):109-133

Gandy, O. (2009) *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage.* Ashgate

Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information.* Minneapolis, University of Minnesota Press

Gardner, D. (2008) *Risk: the Science and Politics of Fear.* Virgin Books

Garland, D. (2001) *The Culture of Control: Crime and Social Order in Contemporary Society.* Oxford University Press

Gibson, W. (1981) *Johnny Mnemonic.* Omni Publications International Ltd

Gill, M. and Spriggs, A. (2005) *Assessing the Impact of CCTV.* Home Office Research, Development and Statistics Directorate February 2005

Gilliom, J. (2011) A Response to Bennett's 'In Defence of Privacy' *Surveillance and Society* 8(4):500-504

Gilliom, J. (2001) *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy.* University of Chicago Press

Gilliom, J. (1994) *Surveillance, Privacy and the Law: Employee Drug Testing and the Politics of Social Control.* The University of Michigan Press

Goffman, E. (1956) *The Presentation of Self in Everyday Life.* University of Edinburgh Press

Goffman, E. (1959) *Asylums Essays on the Social Situation of Mental Patients and Other Inmates.* Anchor Books New York

Graham, S. (2002) *CCTV: The Stealthy Emergence of a Fifth Utility?* Interface Taylor and Francis

Graeff, T.R. and Harmon, S. (2002) Collecting and Using Personal Data: Consumer's Awareness and Concerns. *Journal pf Consumer Marketing,* 19 (4):302-318

Grayling, A.C. (2009) *Liberty in the Age of Terror A Defence of Civil Liberties and Enlightenment Values*. Bloomsbury

Grint, K. (2005) *The Sociology of Work.* Polity Press, Cambridge

Haggerty, K.D. and Ericson, R.V.(2000) 'The Surveillant Assemblage'. In: Hier, S.P. and Greenberg, J. (eds) (2007) *The Surveillance Studies Reader* McGraw-Hill Open University Press

Hansen, S. (2004) 'From 'Common Observation' to Behavioural Risk Management: Workplace Surveillance and Employee Assistance 1914-2003'. In: Hier, S.P. and Greenberg, J. (eds) (2007) *The Surveillance Studies Reader* McGraw-Hill Open University Press

Harper, D. (2011) 'Paranoia and Public Responses to Cyber Surveillance'. Paper Presented at *Cyber-Surveillance in Everyday Life May 2011,* University of Toronto Canada

Harper D. (2008) 'The Politics of Paranoia: Paranoid Positioning and Conspiratorial Narratives in the Surveillance Society'. *Surveillance and Society* 5(1):1-32

Harrison, K. (2012) The App-titude Test: Is Creating a Mobile App Right For You? *Forbes Magazine,* 14/08/2012

Hayward, M. (2009) *Any Colour You Like As Long As It's Any Colour You Like* Purbooks

Hogan, V. Cannon, R. and NicGabhainn, S. (2006) Construction Apprentices' Attitudes to Workplace Drug Testing in Ireland. *Policy and Practice in Health and Safety.* 4(2):43-57

Holden, M. and Lynch, P. (2007) *Choosing the Appropriate Methodology: Understanding Research Philosophy.* Waterford Institute of Technology Repository

Hughes, R. (1998) 'Considering the Vignette Technique and it's Application to a Study of Drug Injecting and HIV Risk and Safer Behaviour'. *Sociology of Health and Illness* 20(3):381- 400

Inglis, T. (2008) *Global Ireland: Same Difference.* Routledge

IpsosMRBI (2012) Social Networking Quarterly Survey May 2012 retrieved from www.Ipsosmrbi.ie/social-networking-quarterly-survey-may-12.html

Irish Council for Civil Liberties (2010) *Experts Call Time on Compulsory Telecoms Data Retention* Press Release 28 June 2010

Jenkins R. (2004) *Social Identity.* Routledge New York

Johnson, D.G and Regan, P.M. (2011) Reconfiguring the House of Mirrors: Narrowing Digitally Mediated Surveillance on Facebook Paper Delivered at *Cyber-Surveillance in Everyday Life May 2011* University of Toronto

Kasper, D.V.S (2007) 'Privacy as a Social Good'. *Social Thought and Research*. 28(1):165-189

Kidwell, R.E. and Sprague, R. (2009) Electronic Surveillance in the Global Workplace: Laws, Ethics, Research and Practice. *New Technology Work and Employment*. 24(2):194-208 Blackwell Publishing

Klein, N. (2000) *No Logo.* Harper Perennial

Komorova, M. and McKnight, M. (2012) 'The Digital Eye in Conflict Management: Doing Visual Ethnography in Contested Urban Space'. *Conflictincities.org* Working Paper No. 28, 2012

Lace, S. (2005) *The Glass Consumer: Life in a Surveillance Society.* The Policy Press, University of Bristol

Komito, L. (2004) *The Information Revolution and Ireland: Prospects and Challenges* UCD Press

Lazar, D. (1998) 'Selected Issues in the Philosophy of Social Science'. In: Seale, C. (ed) *Researching Society and Culture.* London Sage

Lee, N. (2013) *Facebook Nation: Total Information Awareness.* New York Springer

Lett, D. (2007) *Bringing Into Focus the Experience of Public Camera Surveillance.* MA University of Victoria

Lett,D. Hier, S.P. and Walby, K. (2010) CCTV Surveillance and the Civic Conversation: A Study in Public Sociology. *Canadian Journal of Sociology* 35(3):437-462

Lyon, D. (2009) *Identifying Citizens: ID Cards as Surveillance.* Polity Press

Lyon, D (2007) *Surveillance Studies An Overview.* Cambridge Polity Press

Lyon, D. (2006) '9/11 Synopticon and Scopophilia: Watching and Being Watched'. In: Haggerty K.D. and Ericson, R.V. (eds) *The New Politics of Surveillance and Visibility.* Toronto University of Toronto Press

Lyon, D (2003) *Surveillance after September 11.* Cambridge Polity Press

Lyon, D. (2001) *Surveillance Society Monitoring Everyday Life.* Open University Press

Martin, K. and Freeman, R.E. (2003) Some Problems With Employee Monitoring. *Journal of Business Ethics*. 43(4):353-361

MacKinnon (1989) *Toward A Feminist Theory of the State.* Harvard University Press

Manes, S. (2000). 'Private Lives? Not Ours!'. *PC World, 18*(6), p. 312. Retrieved from http://www.pcworld.com/article/16331/article.html

Mann, S. (2004) '"Sousveillance" Inverse Surveillance in Multimedia Imaging'. In: Kerr, I. Steeves, V. and Lucock, C. (eds) *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society.* Oxford University Press

Mann, S. Nolan, J. and Wellman, B. (2003) 'Sousveillance: Inventing and Using WearableComputing Devices for Data Collection in Surveillance Environments'. *Surveillance and Society.* 1(3):331-355

Mathieson, T. (1997) 'The Viewer Society: Michel Foucault's 'Panopticon' Revisited'. *Theoretical Criminology.* 1(2):215-234

Maxwell, R. and Miller, T. (2011) 'Eco-ethical Electronic Consumption in the Smart Design Economy'. In: Lewis, T. and Potter, E. (eds) *Ethical Consumption: A Critical Introduction.* Routledge, New York

Marx, G.T. (1999) 'Measuring Everything That Moves: The New Surveillance at Work'. In: I and R. Simpson (eds.) *The Workplace and Deviance, JAI Series on Research in the Sociology of Work.* MIT

Marx, G.T. (1988) *Undercover: Police Surveillance in America.* Berkeley: University of California Press

McDonald, A.M and Faith Cranor, L. (2008) The Cost of Reading Privacy Policies. *I/S A Journal of Law and Policy for the Information Society 2008 Year in Privacy Issue*

McIntyre, T.J. (2010) *Experts Call Time on Compulsory Telecoms Data Retention* Press Release for Irish Council for Civil Liberties 28-06-2010

McIntyre, T.J. (2009) 'Operation Observation Comes to Ireland'. *Sunday Business Post* April 19 2009

Mennell, S. (1992) *Norbert Elias: An Introduction.* University College Dublin Press

Meyer, S. (1981) *The Five Dollar Day: Labor Management and Social Control in the Ford Motor Company 1908-1921*. SUNY Press

Meyer-Schonberger, V. and Cukier, K. (2013) *Big Data A Revolution That Will Transform How We Live, Work and Think.* John Murray

Meyer-Schonberger V. (2009) *Delete The Virtue of Forgetting in the Digital Age.* Princeton University Press

Miller, D. (2012) *Consumption and its Consequences.* Polity Press

Miller, V. (2011) *Understanding Digital Culture.* London Sage

Monahan, D.M. (2006) *Emotional Labor in Customer Service Work: The Perceived Difficulty and Dispositional Antecedents.* University of Akron

Moore, B (1984) *Privacy: Studies in Social and Cultural History.* Armonk: M.E. Sharp, Inc.

Morozov, E. (2013) *To Save Everything Click Here: Technology, Solutionism and the Urge to Fix Problems That Don't Exist.* Allen Lane

Morozov, E. (2011) *The Net Delusion: How Not to Liberate the World.* Allen Lane

Mosco, V. (1996) *The Political Economy of Communication: Rethinking and Renewal.* Sage London

Mulqueen, M. (2009) 'Securing the State With Soldier Spies: Evaluating the Risks of Using Military Personnel to Gather Surveillance Evidence in Ireland'. *Irish Studies in International Affairs*. 20:121-141

Myers, B.W. (2007) *Shopping the Shopper: Retail Surveillance and Performances of Consumerism.* Southern Illinois University

Nissenbaum, H (2009) *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford University Press Stanford California

Nissenbaum, H. (1998) 'Protecting Privacy in an Information Age: The Problem of Privacy in Public'. *Law and Philosophy,* 17(5):559-596

Norris, C. and Armstrong, G. (1999) 'CCTV and the Social Structuring of Surveillance'. *Crime Prevention Studies.* 10:157-178

O'Hara, K & Stevens, D (2006) *inequality.com: Power, Poverty and the Digital Divide.* Oxford, Oneworld

O'Hara, K. & Shadbolt, N. (2008) *The Spy in the Coffee Machine: the end of privacy as we know it.* Oxford, Oneworld

O'Sullivan , N. (2007) *Every Dark Hour: A History of Kilmainham Jail.* Dublin Liberties

Oxford English Dictionary (2012)

Oxford English Dictionary (2002)

Packard, V (1957) *The Hidden Persuaders.* Pelican

Pamuck, O. (2007) *Other Colours Essays and a Story.* Faber and Faber

Parenti, C. (2003) *The Soft Cage: Surveillance in America From Slavery to the War on Terror*. Basic Books

Parenti, C. (1999) *Lockdown America: Police and Prisons in the Age of Crisis.* Verso

Pariser, E. (2011) *The Filter Bubble What the Internet is Hiding From You.* Penguin

Pavlov, A. (2008) 'Application of the Vignette Approach to Analyzing Cross-Cultural Incomparabilities in Attitudes to Privacy of Personal Data and Security Checks at Airports' In: Zuriek et al. (eds) (2010) *Surveillance, Privacy and the Globalization of Personal Information International Comparisons.* Mc-Gill-Queens University Press

Peppers, D. and Rogers, M. (1997) *Enterprise One to One Tools for Competing in the Interactive Age.* Currency Doubleday

Pinker, S. (2011) *Better Angels of Our Nature: Why Violence Has Declined*. Penguin

Poster, M. (1996) 'Databases as Discourse or Electronic Interpellations'. In: Lyon, D. and Zuriek, E. (eds) *Computers Surveillance and Privacy,* Minneapolis University of Minnesota Press

Pridmore, J (2012) 'Consumer Surveillance Context, Perspectives and Concerns in the Personal Information Economy'. In: Ball, K. Haggerty, K.D. and Lyon, D. (eds) (2012) *Routledge Handbook of Surveillance Studies.* Routledge

Pridmore, J. (2010) 'Loyalty Ambivalence in the United States and Canada: The GPD Survey, and the Focus Groups, and the Context of Those Wonderfully Intrusive Loyalty Cards'. In: Zuriek, E. Harding-Stalker, L.L. Smith, E. Lyon, D. and Chan, Y.E. (2010) *Surveillance, Privacy and the Globalization of Personal Information.* McGill-Queen's University Press London

Pridmore, J. (2010) 'Reflexive Marketing: The Cultural Circuit of Loyalty Programs'. *Identity in the Information Society* 3(3):565-581

Rayner, T. (2001) 'Biopower and Technology: Foucault and Heidegger's way of thinking' .*Contretemps* May 2001

Regan, P.M. (1995) *Legislating Privacy: Technology, Social Values and Public Policy.* University of North Carolina Press

Rice, A. (2013) 'We Are All Friends Nowadays: But What is the Outcome of Online Friendship for Young People in Terms of Individual Social Capital?'. In: Fowley, C. English, C. and Thouesny, S. (eds) *Internet Research, Theory, and Practise: Perspectives From Ireland*. Research Publishing.net

Ritzer, G. and Jurgenson, N. (2010) 'Production, Consumption, Prosumption The Nature of Capitalism in the Age of the Digital 'Prosumer''. *Journal of Consumer Culture* 10(1):13-36

Ritzer, G. (2007) *Blackwell Encyclopedia of Sociology Online* retrieved from www.sociologyencyclopedia.com (Accessed 15/09/2012)

Rose, N. (1985) *The Psychological Complex.* London Routledge

Rowe, M. (2008) *Introduction to Policing.* London Sage

Sassen, S. (1996) 'Cities and Communities in the Global Economy: Rethinking Our Concepts'. *American Behavioral Scientist* 39: 629-639

SCAN (2009) *A Report on Camera Surveillance in Canada Part One,* Surveillance Camera Action Network found at www.surveillanceproject.org/projects/scan accessed 22-01-2013

Schilling, C. (1993) *The Body and Social Theory.* Sage

Schneier, B. (2008) *Schneier on Security.* Indianapolis, Wiley

Schneier, B. (2003) *Beyond Fear: Thinking Sensibly About Security in an Uncertain World.* Copernicus Books

Sewell, G. (1998) The Discipline of Teams: The Control of Team-Based Industrial Work Through Electronic and Peer Surveillance. *Administrative Science Quarterly,* 43(2): 397-428

Sheller, M. and Urry, J. (2003) Mobile Transformations of 'public' and 'private' life. *Theory, Culture and Society* 20(3):107-125

Siggins, L. (05/04/2011) 'Mayo Garda Comments Investigated' *Irish Times*

Simms, A. (2007) *Tescopoly: How One Shop Came Out On Top and Why it Matters.* Constable London

Simon, J. (2007) *Governing Through Crime How the War on Crime Transformed American Democracy and Created a Culture of Fear.* Oxford University Press

Sofsky, W. (2007) *Privacy A Manifesto.* Princeton University Press

Solove, D. (2011) *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press

Solove, D. (2008) "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy* Harvard University Press

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

Stalder, F (2002) 'Privacy is not the Antidote to Surveillance'. *Surveillance and Society* 1(1) 120-124

Steeves, V. (2003) 'Reclaiming the Social Value of Privacy'. In Kerr I, Steeves V, &Lucock C, (eds) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society.* Oxford University Press

Taylor, F.W. (1911) *The Principles of Scientific Management* Project Gutenberg Press (2004)

Toffler, A. (1980) *The Third Wave* William Morrow

Trentman, F. (2004) 'Beyond Consumerism: New Historical Perspectives on Consumption'. *Journal of Contemporary History*, 39(3): 373-401

Turrow, J. (2006) 'Cracking the Consumer Code: Advertisers, Anxiety and Surveillance in the Digital Age'. In: Haggerty, K. and Ericson, R.V. (eds) *The New Politics of Surveillance and Visibility.* University of Toronto Press

Van Dijk, J. (2006) *The Network Society* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Van Grove, J. (2012) 'Your Address Book is Mine: Many Iphone Apps Take Your Data' found at www.venturebeat.com/2012/02/14iphone-address-book accessed 20-03-2013

Veal, W. R. (2002) 'Content Specific Vignettes as Tools for Research and Teaching'. *Electronic Journal of Science Education, 6*(4). Retrieved from http://ejse.southwestern.edu/article/view/7687/5454

Veblen T. (1973) 'The Theory of the Leisure Class'. In: Grusky, D.B.(ed) (2001) *Social Stratification in Sociological Perspective.* Westview Press

Wacquant, L. (2008) *Urban Outcasts: A Comparative Sociology of Advanced Marginality.* Polity Press

Wacquant, L. (2008) Ordering Insecurity: Social Polarization and the Punitive Upsurge *Radical Philosophy Review* 11(1):9-27

Wacquant, L. (2006) 'The 'Scholarly Myths' of the New Law and Order Doxa'. *The Socialist Register* 42(1) 93-115

Wacquant, L. (2004) *Punishing the Poor: The Neoliberal Government of Social Insecurity.* Duke University Press

Walby, K. (2005) 'How Closed Circuit Television Surveillance Organises the Social: An Institutional Ethnography' In: Hier, S.P. and GreenBerg, J. (2007) *The Surveillance Studies Reader.* Open University Press

Wall, D. (2006) 'Surveillant Internet Technologies and the Growth in Information Capitalism: Spams and Public Trust in the Information Society'. In: Haggerty, K and Ericson, R.V. (eds) *The New Politics of Surveillance and Visibility,* University of Toronto Press,

Warren, S. and Brandeis, L (1890) 'The Right to Privacy'. *Harvard Law Review*, 4(5)193-220

Watt, J.(2009) *Electronic Workplace Surveillance and Employee Privacy- A Comparative Analysis of Privacy Protection in Australia and The United States.* Queensland University of Technology

Weber, M. (1921) *Economy and Society: An Outline of Interpretive Sociology* Translation by Roth, G. and Wittich, C. (1968) University of California Press

Welsh, B.C. and Farrington, D.P. (2008) 'Effects of Closed Circuit Television Surveillance on Crime'. *Campbell Systematic Reviews*, 2 December 2008

Westin, A. (1967) *Privacy and Freedom.* New York U.S.A. Atheneum

Wood, A. (1998) 'Omniscient Organizations and Bodily Observations: Electronic Surveillance in the Workplace'. *International Journal of Sociology and Social Policy.* 18(5):136 - 174

Yar, M. (2006) *Cybercrime and Society.* Sage London

Zimmer, M. (2008) 'Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine'. *Journal of Business Technology and Law*, 3(1), 109-126. Retrieved from http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1094&context=jbtl

Zuboff, S. (1988) *In the Age of the Smart Machine: the Future of Work and Power.* Harvard, Basic Books

Zurawski, N. (2011) ‘Local Practice and Global Data: Loyalty Cards, Social Practices, and Consumer Surveillance’. *The Sociological Quarterly*. 52:509-527

Zuriek, E. Harling Stalker, L.L. Smith, E. Lyon, D. and Chan, Y.E. (2010) *Surveillance, Privacy and the Globalization of Personal Information International Comparisons* McGill-Queens University Press

## Appendix 1 Participation Consent Form

Security, Privacy and Technology: Contemporary Irish Perspectives

Participation Consent Form

You are asked to participate in a post graduate research study conducted by Kenny Doyle, a postgraduate research student from the Centre for Social and Family Research, dept of Applied Arts at Waterford Institute of Technology, Ireland

The study is entitled 'Surveillance, Privacy and Technology: Contemporary Irish Perspectives'. There is an information sheet with this form, explaining what the study is all about and what I hope to do with this study. Kenny will read it to you and please ask him to explain anything that you do not understand on the information sheet.

Kenny Doyle is under the supervision of Jonathan Culleton at the Centre for Social and Family Research, WIT. If you have any questions or concerns about this research or information contained in this form please feel free to contact Jonathan Culleton at jculleton@wit.ie

Purpose of the study

The purpose of the study is to explore with people currently residing in Ireland, their knowledge levels regarding personal data, and how it can be used and misused with the aim of exploring the level of public knowledge regarding surveillance and its effects on individual citizens.

Procedures

If you volunteer to participate in this study, we would ask you to do the following things:

participate in a one- on – one interview, lasting about sixty minutes with the researcher
be open and honest as you can in answering the questions asked
what you say in the interview will be confidential and every possible measure will be taken to ensure that you will not be identified. The researcher will know only your identity and your name will not be used when writing up the research
you may refuse to answer questions you don't want to answer and still remain in the study

Potential Risks and Discomforts

Participation in this research is completely voluntary. This means that if at any point you wish to end the interview and/ or withdraw from this study you may do so.
Also if at any point the researcher feels that you are emotionally unable to participate they may also end the interview and/ or your participation in the study. Your welfare will always be the main concern.

Potential benefits of the research

This research seeks to gain an understanding of individuals own experiences, knowledge and opinions on the issue of surveillance, and therefore will seek to inform future debates on security and data protection, from a citizen- centric perspective.

Voluntary nature of Participation

You will not be paid any money or receive any reward of any kind for participation in this research. Also, please be aware that if you decide not to participate in this study it is not a problem, it is completely voluntary.

Confidentiality

Every effort will be made to ensure confidentiality of any identifying information that is obtained in connection with this study. During the interview you will be recorded by voice recorder. This information will then be transcribed and thereafter will be placed in a password- protected file so that it cannot be accessed by anyone other than the researcher. The recordings of the interview will be kept for the duration of the research and the information you give will be used only for the purposes of this project.
Your name will be changed in order to protect your identity and the researcher will have only one document, password protected, on computer stating your actual name and the 'new' name so that the only person who can identify you is the researcher. None of these files will be printed in paper format. Should it be necessary to do so for any unforeseen reason the file will be stored in a locked filing cabinet and immediately shredded once it has served its purpose.

Rights of Research Participants

You may withdraw your consent at any time and discontinue participation in the study. This study has been reviewed and received ethics clearance through the Waterford Institute of Technology.

Consent signature of research participants

I have read the information provided for this study 'Security, Surveillance and Democracy: Contemporary Irish Perspectives'. My questions have been answered to my satisfaction, and I agree to participate with this study. I have been given a copy of this form.

Signature of participant

_____ _____

date

Name of participant (please print)

_____

Signature of witness/ researcher

_____ _____

Name of witness/ researcher date

_____

## Appendix 2 Interview Schedule

### 1. Overview of terms

Do you know about or have you heard of any of the following

-cookies

-Global Positioning Systems (GPS)

-Radio Frequency ID (rfid) tags

-cctv cameras

-Biometrics

-Facial Recognition Systems

-Data Mining of Personal Data

-Automatic Number Plate Recognition

for answers of yes ask respondent to explain their understanding

### 2.Surveillance

What do you understand surveillance to be?

How would you feel if you were under surveillance?

### *3. Privacy*

What do you understand Privacy to be?

Do you think it is important?

How would you feel if someone known or unknown to you read your emails?

Do you think we have more or less privacy now than we did in the past?

Would you be prepared to give up some of your privacy for security reasons? ie to prevent terrorism or crime.

Would you be prepared to give up some of your privacy for financial reward?

### 4. Data

Have you ever thought about the digital trail you leave behind? Think about as many sources as you can that leave behind a digital footprint.

explore with respondent any potential uses of these data trails

### 5.Internet Use

How often do you use the internet?

Do you use social networking sites? which ones? Have you ever changed the privacy settings?

Do you use a search engine? which one?

How do you think (social networking site) makes money?

How do you think (Search Engine) makes money?

### 6.Resistence

Have you ever refused to give information to a company/website/government agency?

Have you ever knowingly given misleading or incorrect information to a company/website/government agency?

Have you ever asked a company/agency to remove you from their records? or to show all records they have pertaining to you?

### 7.Employment

How do you feel about being watched in work?

-video cameras

-performance objectives

What would you think if you found out that your employer was watching you outside of work? -facebook etc.

How would you feel if you had to complete a drug or alcohol screening in work?

**8.CCTV**

What do you think about video cameras in public places?

**9. Vignettes**

Now I'm going to tell a few fictional short stories and I'll ask your opinions afterwards.

Sean left home to go to work, as he drove towards town he passed a Garda traffic corps car which recorded his registration, his car tax situation, the direction he was travel ling and the time.

Do you think his privacy has been respected?

Do you think law enforcement agencies should have access to such information?

Mary was shopping on the internet for a new pair of shoes, she went to site a.com and found a pair she liked, later on she found and bought the same shoes at a lower price on site b.com. When Mary went on to site a, her activity on the site was tracked for marketing purposes, a report was compiled which showed what items Mary had looked at, how long she looked at them, and which site she ultimately used to purchase her shoes.

Do you think her privacy was respected?

If such tracking improves quality of service do you approve of it?

Mshops regularly in the same supermarket, she recently accepted a loyalty points card which she presents at the till each time she is shopping. By using the card she gets a discount on her purchases, in return for this the supermarket gets a detailed list of her preferences and they can compile a profile of their customers. The information held by the supermarket is then sold on to other marketing companies.

Respondent details
Do you use the internet?
Do you have a bank account? Credit Card?
Do you have insurance? Do you drive?
Do you have a mobile phone?

## Appendix 3 Sample Interview

I-interviewer, R-Respondent

I: So firstly again thanks for coming to see me, what I'm going to start with I'm just going to read out and go through a list of ehm technologies just to see if you have heard of any of them. Now generally people won't have heard of most of these so if you don't recognise any of them don't worry about it

R: No problem I won't have heard of many of them I'm sure,

I: So the first one is in the context of the internet; cookies would you have any idea what they are?

R: It's ehm, I don't know exactly, I have seen and heard the term, it's something that eh it can, not track but it remembers what sites you have been on is that it?

I: yeah, that's close to it, it's pretty much exactly it actually, what about GPS systems or global positioning systems?

R: I don't know anything about them, I know I have it turned off on my phone (laughs) I don't really know that much about it, I don't have one of those eh what do you call it sat navs or anything like that in the car or anything but eh no I don't know alot about GPS systems

I: did you purposefully turn it off on your phone

R: somebody told me to turn it off, or that you can be tracked by all sorts of people or whatever you know, but I don't know exactly what it is but I know it's.. some people use them if they get lost or you know to spot themselves on a map or whatever but it's ehm I just turned it off because this guy told me at work, he said you shouldn't really have that on he's a very security conscious kind of a guy

I: mm right ok, sure we'll come back to that in a bit but for now have you ever heard of Radio Frequency ID tags or RFID?

R: Never, No

I: People generally don't know what they are, ehm have you ever heard of smart CCTV cameras?

R: Smart CCTV no, I know what CCTV cameras are

I: Do you know where there are any in operation?

R: would they be ones that are out in the public eh?

I: mm

R: yeah there's a few around New Ross town, the council have them I work in Wexford General Hospital and we have them all over the place down there, I work in the orderly security department down there

I: So would you use CCTV much

R: We do use CCTV all the time down there yeah for burglaries in the hospital, for accidents out in the car park,

I: Right, and I suppose drunks coming in to the emergency unit I assume they would be closely watched?

R: yeah well it doesn't pick up any sound, but yeah you would keep an eye on particular areas

I: For threatening behaviour

R: yeah but they get moved around a bit depending on the area and their use like eh the waiting area in casualty would be one where there's one constantly on it, ehm outside of the maternity unit and the paediatric unit, not on the ward itself but just on the entrance and exit so that if somebody tried to snatch a baby or a child there's constantly a camera on them.

I: Oh right ok have you ever used CCTV footage would it always kind of be after the fact something had happened or would you

R: No sometimes if there was eh, if there was an aggressive patient or a psychiatric patient that eh you see we can't make anybody stay in a particular area down there so if there was eh a psychiatric patient in particular that was wandering around maybe going out for cigarettes then you would keep an eye on them on the cameras so as not to antagonise them by following them around you know

I: I get you yeah, so it's like keeping control of them from a distance

R: or supervising them keeping tabs on them yeah

I: ok have you ever heard of biometrics

R: no I may have heard the term but I have no idea what it is

I: Ok em and what about facial recognition systems

R: eh I know what facial recognition systems are but they are similar to fingerprint type thing, but I've never seen one in operation

I: yeah

R: Oh I have actually I saw one in operation in what airport was I in, out in Charles De Gaulle they have that kind of thing where you have to turn around now and it has everything,

I: oh right I've never seen that one, do you know facebook use facial recognition have you ever seen that?

R: no, oh yes they do on the photos, is this you or...

I: yeah

R: that they can guess people that look like you in photos and eh to save you tagging, jeez I didn't know that I thought it was eh you know when you go into the thing

I: well it is that as well, and it's funny you said about Charles De Gaulle because in Schipol in Amsterdam they have a system called trivium

R: actually sorry it was Schipol because I fecked up my travel plans the last time, normally I eh, my partner is from Brazil and eh we usually go through Charles De Gaulle but this time it was cheaper to go through Amsterdam and that was where I saw it

I: have you ever heard of data mining of personal data?

R: No

I: ok and have you ever heard of an automatic number plate recognition system?
R: would that be something similar to the toll bridge going up to the airport something like that?
I: yeah, well they use them there
R: like if you don't get a ticket, it recognises your number because it did happen to me once that I went through it without, I thought I had the ticket already got and I got a letter a couple of days later saying I went through the toll bridge without paying and my number was on it so
I: and do you know of anywhere else where it's in use
R: mm no are you gonna tell me all these things where there used when we are finished
I: yeah of course no problem, so we'll talk a little bit about surveillance in general, if I was to ask you what you understand surveillance to mean if I said such and such a person was under surveillance?
R: probably the general one you know, the kind of spy and espionage thing where you know ehm somebody would be watching your movements or tracking your online activity or possibly your phone calls or whatever
I: do you think that happens much
R: yes
I: at what kind of level do you think?
R: I would say... you mean at what level of severity or what kind people?
I: I mean how often
R: I would say it on all the time with certain people, I know... I'm very politically active em and I know that my apartment has been watched, eh I know that I've been stopped numerous times and asked questions about various protests I was on ehm sometimes I have thought that my facebook has been hacked, once it was hacked and I lost my account, em I do think the level I hear of people whose accounts have been hacked is slightly exaggerated but unless it was individuals doing it who knew there passwords or whatever but I would say even though my facebook is set to private and you can't see anything on the public if you do a search on it there are people who would have access to it and probably would look in on it from time to time, the levels of privacy we say are there are actually in existence em phone calls I don't know I'm sure there's lots of ways

of listening to phone calls through scanners and the like of that I don't know if I ever, I have I was in the company of somebody who had one of those police scanner things so I know that it goes on and I'm sure that if those are accessible to the general public then people who access to them have much more sophisticated stuff as well
I: yeah em how would you feel if, like you mentioned that you thought you were being watched or your house was being watched, how did that make you feel?
R: It's un-nerving, it's un-nerving and I do remember being in the socialist workers party office in Dublin one day and two guys who the lads in the office told me were from the special branch were waiting across the road in a car and it did feel a bit like what have I done you know, I mean I'm only on a protest against austerity budgets and stuff I'm not a threat to state you know (laughs) or perhaps I am I don't know
I: so you see surveillance like that, there is some kind of implication of guilt?
R: mm
I: that you said what have I done to deserve this is exactly what you said
R: exactly yeah
I: mm and when you mentioned your house being watched, who, did you think that it was the police?
R: yeah, I assume it was the police, I doubt it was another political party or whatever, I don't think they would be too interested in what I'm doing but yeah em now it hasn't been for years but em and I never involved in the republican movement and I would be totally opposed to what went on in the republican movement but I did have my house searched once
I: really
R: yeah, years ago when em I forget his name but the border fox was what he was called
I: yeah Dessie O'Hare
R: yeah they searched the house that time, as if he's gonna be in my house, I'd probably be on totally the other end of the political spectrum to what he would have represented you know
I: yeah
R: but probably because I was active in politics at the time in left wing politics
I: and how long ago would this have been

R: probably about, it would have been in the eighties, I mean I was still living in my mothers house I was probably only about twenty or something, you know

I: yeah

R: he wasn't there anyway (laughs)

I: so they didn't find him holed up in New Ross, em ok so we'll talk a little bit about privacy, I think we'll come back to some of that stuff you were talking about it's very interesting, but what would you understand privacy to be?

R: eh again in relation to surveillance or?

I: well just in general

R: well in the context of the internet I would have hoped that privacy means that my friends or people that I am interacting with aren't having what they say to me monitored nor is what I'm saying to them being monitored but I don't actually pay much attention to it I'm not obsessed with it and I'm of the opinion that anything I'm saying is not that important and I just go ahead and say whatever I have to say and probably would encourage others to do it as well but after this discussion so far you're probably making me a little bit more aware of this stuff and I'm getting a bit paranoid!(laughs) but em no I would expect privacy to mean anything that you would expect it to mean that any of your online activity or your phone calls or anything is private and that others don't have access to it but I don't believe that that's the case, I'm sure that, well I think it is the case that every text message you send is kept on record and they, I mean I've seen cases legal cases where stuff has been mentioned about tracking people and mobile phone activity and stuff like that, remember that guy in Wicklow that killed his wife

I: yeah it's probably the most famous one I think

R: yeah so I think that if anyone is to think that anything electronic is private then there probably a bit in the sky,

I: What do you think happens if privacy is lost?

R: I would say if privacy is lost I would say that there is definitely a sense of paranoia and eh a lack of basic freedom to interact as you would if you weren't being eh monitored or if there was total privacy it probably would stop the normal flow of communication but I'm not sure I'm not an expert in any of this I'm only saying what's in my head you know

I:  the next question I'd often ask is do you think we have less or more privacy now than we did in the past but I think you've kind of answered it already

R: we have less, it's very obvious that we have less because we are depending on much more artificial means of communication as well, we're not communicating as much face to face as we were you know

I: mm ok and eh would you be prepared to give up some of what you value as being privacy for security reasons, so if you were told like you mentioned a threat to the state, be it terrorism or organised crime, would you be prepared to give up some privacy of you were told we could stop this

R: no because I don't, I wouldn't see the privacy of an individual as having anything to do with eh monitoring terrorists or anything like that I think that there's definitely a history of monitoring terrorist groups outside of interfering with your average joe soap on the street you would have had it in the North where both sides the loyalists and the nationalists would have had there groups infiltrated by various people and that and I'm sure the whole phone tapping thing and that but I'm sure that ehm I don't see how me giving up any of my privacy could make any difference into monitoring someone else, I mean I don't see how me allowing someone to see my photos on facebook could lead to the capture of em.....

I: Osama Bin Laden

R: Osama Bin Laden or whoever do ya know,

I: at the same time would you be prepared to give up elements of your privacy for financial reward, so say if we use the facebook photo example again, that if you allowed facebook to publish your photos outside of your own circle and they gave you credits or money or something, would you be ok with that?

R: no

I: no

R: no

I: ok that's a straight answer I suppose

R: (laughs) but I'm sure people would, I'm sure people would be eh, because people are motivated by money, but eh I don't, I don't like the idea that they would give you financial reward for invading your privacy, you're into dangerous territory again then,

you don't know where it's gonna stop, I mean they might say let us have a look at your text messages as well

I: I suppose it would kind of depend because the one thing I have kind of learned is that what one person would see as being totally private, another would say ah sure I don't care who knows that

R: mm I do feel a bit like that, I mean I don't mind because most of what I say is for public consumption, I don't use my facebook to keep in touch with my family, or friends either, I have alot of my friends that are on it but anything that's on it is of a political nature and is generally for public consumption and I want people to see it, I use facebook as a propaganda tool for my work you know, it's not eh even though I set it to private there's over a thousand people who are on it most of whom I wouldn't know, and *I know* for a fact that there's a number of those who aren't real people and that they would be just monitoring it or having a nose around, but to come back to the photos it might be fine for you to say yeah they can have access to my photos but if I'm in your photos

I: exactly

R: it's not something that I'd like to think that somebody could be selling photos of me in them as well

I: ok yeah..... this is again something we have touched on a little bit, we were talking about like the internet and phones and so on if you've ever heard of the phrase a carbon footprint,

R: mmm

I: if you were to think about a digital footprint, and think about all the ways that you leave a searchable record behind you

R: yeah

I: could we maybe even tease that out, like you mentioned the internet and your phone, what kind of data do you think you could get from them

R: what data am I leaving behind, like a permanent record

I: yeah or even if  you can think of any other types that can leave a permanent record

R: yeah ehm I don't, I don't know exactly but I know that anytime that eh that you want to go on to a certain type of website or whatever that you've got to leave your email

address and you know all this kind of stuff and I often wonder well why can't I just log on to this site without having to give all this stuff but (laughs) I have started using a separate email address just for registering on sites so I don't use my primary email any more for registering, just particularly for that reason that I don't want to get a load of spam, from them you know, I don't know if when you send a text message are you leaving a permanent record but again you are leaving them there yeah, and what was the question you were asking me again what are the implications for leaving it behind or?
I: well first I suppose even if we just list all the other things you do that would kind of leave a record
R: well everything you do, you're talking specifically about technology is it? or in general
I: well in general stuff in your everyday life
R: yeah of course every time you've got to you know, you mentioned it yourself earlier you know about the household tax thing I mean even if you go into your local council which you can do you've got to give all your details, PPS number, size and type of property, how many people are living in the house and everything, and I feel that's a bit of an invasion of the privacy we're talking about, but that's a permanent record to be used in the future for other taxes and stuff and something that was pointed out to me today which I really didn't register before was that people who live in local authority homes are exempt from the household tax at the minute, but they're already on record because they're tenants of the council so they are already known but wherever you go even if you want to join a gym, they are getting all of your details from you, you've got you know to get a phone you need two utility bills you know all of this kind of stuff you know
I: Yeah
R: where was I the other day and they asked me for my drivers licence, I can't remember now, It'll come back to me in a minute but they asked me for my drivers licence to prove who I was
I: yeah em and then as well if we think of stuff like text messages and data, that can be retained, I mean purchasing data as well, I mean if you buy something online or use a laser card of anything like that

R: yeah
I: could you think of any ways that if this type of information is kept that it could be used at a later date
R: no I can't, I'm sure there's lots of them, but the one about the, the one that's in my mind is obviously the household tax which will be used again to hit people with this broadcasting tax that they are talking about and other hidden taxes and charges in the future, I don think that if you register for any of those type of sites and you leave that permanent record, you're much more easily traceable to you know be hit with more spam from the government say,
I: yeah
R: with the tv license say, as it won't be my name on it I don't have a tv license and I refuse to get one, but I always receive notification for the occupier with my address underneath it, but I don't engage with that at all because until they have my name in the tv licensing in the post office then they can't charge me with not having one
I: ok and I suppose what you're saying is right because if you've seen over the last week how quickly the septic tank charge dropped form fifty to five like as I say it's not about getting the charge in it's about creating the register
R: yes
I: and that would kind of feed in to what you're talking about, so em how often would you use the internet
R: oh I am an avid user of the internet, everyday and several times of the day I use it on my phone everything,
I: right
R: I'm terrible
I: it's actually become a bit of a silly question because everyone says everyday, of course I use the internet everyday
R: I'm always,... emails come directly to my phone and yeah, probably too much is the answer
I: ah I'm not sure, ehm do you use social networking sites I know you use facebook
R: facebook yeah is the only one I use, I want to use, I actually have a twitter account I want to use but I don't know how to tweet properly

I: I've never got into twitter myself
R: I did have for a while somebody tweeting on my behalf because I couldn't use it, so a friend of mine I got him to put up a few messages a few tweets but I didn't have too many followers and I didn't follow too many people and I didn't find it interesting enough or engaging enough for me, you know a hundred and sixty characters is not enough for me to read you know
I: there's a limit to what you can say in that
R: but even in the way that there's a limit to what you can and read and the information you can get as well, em so I wasn't really... but facebook I find facebook quite good and em but it's worrying because I do hear lots of people saying how how em every time they change their settings, the other day I got bombarded with messages from google saying they were changing their privacy settings so I didn't even read them and I just deleted them, basically I didn't even know what they are talking about I mean I'm getting an email what are you gonna do you know
I: yeah
R: so I didn't read I should have read it you know but I deleted it, I got three email in the one day from them
I: so you felt that they were kind of bombarding you with stuff
R: yeah I did I did, and I actually felt at one stage that I was going to write back and say if you keep sending them to me I'll just switch to hotmail or something else you know,
I: yeah and I suppose as well I kinda got from what you said there that kind of em even if they were contacting you it was just an email and you couldn't reply
R: it would just bounce back
I: so it wasn't as if you had any input, you kind of mentioned as well about the privacy settings, you changed the one on facebook you said,
R: mm
I: would you be kind of privacy conscious online
R: em only to the extent that I don't want my ex-girlfriend to see what I'm doing
I: right (laughs)
R: even politically (laughs), they are set to private but there are over a thousand people who have access to it mm and even some stuff I would leave it, even if there are some

photographs that I had taken myself I usually leave them just open but there usually just of birds and trees and stuff

I: and you were saying that you reckon that some people have made friends with you on facebook that don't exist

R: well I know that there I know because a couple of them I had a little check I don't know if you do it or if someone else does it but you know have a little look at there wall first of all and I'm always weary of people who have a small number of friends who I don't know ehm and then having limited similar interests to me so normally I accept them have a little snoop around and then delete them so that has happened quite a bit

I: Right

R: but one particular one I got a while ago was somebody pretending that they were in New York, he may have been in New York I doubt it but he had befriended a huge amount of left wing people in Ireland and he actually sent me a couple of messages saying that he was coming to Ireland and he was looking for places to stay and whatever and this was quite bizarre you know

I: yeah

R: like eh how did he even know these things, but he was obviously working off of I mean I'm not saying I'm well known but people know who I am in politics and this guy was obviously compiling a list of people on the left and having a little snoop around their pages so I deleted him and I actually did warn other people not to add him, I also got an email about somebody who was adding people as well a different person who was adding people as well so em just to hack into there accounts and he had actually hacked into two friends accounts and messed them up in some way

I: and was that for political

R: again for political things, I mean the left is small enough in Ireland without those feckers hacking in you know (laughs)

I: and you mentioned about a dossier or a file being made up about certain political groupings how easy do you think or how difficult it is to do that these days

R: very easy and I did speak about this at a meeting recently in Dublin that there was about sixty people in the room and I said that we would be foolish to think that there's not somebody in this room who is a member of the special branch or the police force or

is some way linked to state apparatus because eh the left would be quite open and eh if anybody shows an interest then of course they would be welcomed with open arms and I don't know if you saw -you probably did because you seem to be very aware of what's going on – about the policeman who was involved with the shell to sea

I: In Galway I had heard about that yeah

R: So it was around that time that we were talking about this and I said well there's probably somebody here that's a member of the police force and we don't know because we would be going on quite well organised protests eh with various left wing issues, and we would be protesting outside the dail and stuff like that

I: and what kind of reason would you think that

R: obviously political reasons I mean I'm sure they don't want eh... revolutionaries to be plotting the downfall of the government (laughs) in secret, not that we'd be plotting in secret we'd be very open about what we'd like to see changed in our society but there's a paranoia on the right in Irish politics that in some way revolution can be built in Ireland I'd be less optimistic because even though I'm trying to build a revolution in Ireland I'd be less optimistic than the right, that it can be done, but definitely there would elements in the security services that would want to keep an eye on what's happening just to make sure that eh the dail wasn't stormed for instance, you remember that there a couple of years ago there was a protest outside the dail and some people ran in to the plinth now that wasn't organised

I: and they were battered straight back out again

R: it was actually a totally spontaneous thing and they actually just wanted to go in and sit on the plinth and have a sit in in there there was no .....

I: plan to get inside

R: thoughts of getting in to the dail which was an irrelevant action in my thought, but I did actually find out which I had never even thought of it but there are armed security in the dail I never knew that

I:yeah

R: plain clothes security, I never knew that and I had been in the Dail a few times

I: and do you think that it's only politics of a certain type like..

R: no and it's definitely not just the left because there would be a growing right wing

eh extreme right wing fascist element as well
I: I didn't know that
R: there's a good cell of them in Kilkenny in the city and Limerick as well in the city that's where their two key people are and there's a growing element you also might have heard of the free man group,
I: I've heard of them alright
R: now they would have some very right wing tendencies as well, they em one of the strong things they would be opposed to would be immigration into Ireland
I: I have seen with some of the free man groups some the ehm almost imagined Celtic identity
R: yeah
I: this almost pure celtic people
R: Their whole eh ethos would be based on Brehon law and you know to be honest with you they'd probably nearly want us living back in Crannogs (Laughs) but they challenge the law alot using this thing of Black's law
I: yeah that's more how I had heard of them
R: well it's wrong and it's all based on this individualistic, and the whole statutes thing is nonsense you know
I: em yeah, I've never come across anyone in the course of doing this who has experience of focused surveillance so I am quite interested in it so the kind of stuff like the facebook friends, and you did mention people looking at your house as well, what other types and ways like say for argument sake if I worked for the police, what ways do you think I could go about finding information about you if I wanted to
R: well politically you see I'm very open so there's nothing hidden so em I would be very hesitant to discuss particular elements of politics with you, until I knew you really well, but I would have to develop a trusting relationship with somebody before I would start taking about certain things
I: or future plans
R: well I'm not planning an armed overthrow of the government or anything like that, so you wouldn't be talking about stuff like that but even just organising big protests against say the IMF. Like we had a big protest against the IMF outside the Merrion hotel when

they were staying there, there was more police on the protest than there were actual protesters and there was about eight hundred or a thousand people so how would I go about ehm I don't go about it usually, I mean I don't mind I mean I'm quite open to confronting people if they have an issue with my politics I'll take it on head on and try to argue my point with them but em I dunno I'm going around with like the mirror on looking under the car just yet I don't see that I'm under any threat other than I am aware that people would be snooping around on my facebook, political opponents possibly I might be making it a grander thing than it is you know

I: em yeah out of interest as well, when you're on protests and you say that there's kind of more police than people there, do the police ever video tape you

R: em oh sure they have helicopters overhead and everything usually even if there's only eight hundred there's usually the old eye in the sky em they may not video but there is always somebody videoing whether it's a journalist or a policeman or whatever

I: and have you ever as an organisational way of looking at it filmed the police back filming you?

R: yeah particularly at the student demo at the department of finance was that the year before last,

I: that was the one that got fairly rough

R: yeah where a friend of mine was hit on the head by a bean garda you might have seen the video and he was carried out and while he was on the ground he was kicked by a policeman but em yeah we filmed them back that day

I: and do you think you filming them can alter their behaviour in any way or do you think it gives you any power

R: yes it does, if it's done at the right time, if they are aware of it but sometimes if it escalates if violence escalates on a demonstration yeah the police lose their head and they lose control you know, now I know they're getting more training in crowd control as the recession deepens they're getting more training in how to control protests and that but yeah it definitely does when you've got the camera in their face they are different. A very clear demonstration of that was at Occupy Wall Street when they blocked off the park I can't remember the park they were in

I: Zuccoti Park

R: yeah that's it it's your young memory, eh but I remember when they tried to get back in when the protestors tried to get back in a few days later and they blocked off one of the streets to it and started initially to beat the protestors but when they were aware that there was a huge media presence with cameras they just put the barriers aside and let them through you know, but they let them through in an ordered way one by one you know, so definitely it turns the tables on them a little bit

I: yeah it's something that often comes up, counter surveillance is what they call it, the most famous example would be the Rodney King footage, but I was interested because if you ever look at any footage from the anti-globalisation protests in the US or Britain you'll always have police filming what's going on so that they can identify people at a later stage but what you also have is protestors filming the police and this is again if you remember the man who was pushed over by a policeman at a protest in London and he died after it, that was filmed by a protestor and not by the police, and you do have cases where, and the police do this as well where you can kind of selectively manage what they put out,

R: yeah

I: like one example in Britain is a woman who wound and wound and wound and said deplorable stuff to a policeman and eventually he thumped her which is what she wanted him to do, but her friend turned on the camera at a particular time to just catch him thumping her. The police do as well like in the US when the police have cameras at the front of the car they know where the blind spots are so the footage isn't always reliable

R: well we always thought that on the protests we're not the ones who show up in riot gear you know, we're not showing up for a riot we're coming to openly and democratically use our right to protest and normally it's the reaction because of chanting against whatever it would be and people get excited about that you know there can be a kind of a frenzy built up and then if there's anyone even pushing from the front you can be liable to get a wallop you know

I: yeah and have many protests you've been involved in ended up getting violent?

R: I was, I wasn't involved in it but I happened to be on it was the poll tax riot in Britain, I was on that because I was living in Britain at the time and that was very strange because that was one of the most well behaved and carnival like protests I have ever

seen it was fantastic there was loads of music and there was people dancing you know it was a nice day, ironically the thirty first of march, the date there's a registration for our poll tax is due, on a Saturday as well. There was a million people on that protest the majority of whom there was a small group of anarchists who decided to have a little go at the police and that's where that all spread from, but the police totally over reacted

I: but from their point of view with that number of people, if it was to kick off they'd be screwed

R: yeah well they thought that we were going to burn down parliament

I: even if you look in Britain over the summer with the riots where they were caught by surprise and they were stretched and some claimed that law and order did completely disappear, just to back to the internet, do you use a search engine?

R: Google

I: and have you ever thought about how Google makes its money

R: no, I haven't but they do have ads on their page, do they even have ads on their page anymore, I don't even know whether they do or not

I: have you ever noticed what kind of ads are there?

R: no I have not, I'm not sure they have ads on there, I just have it on the page where there's nothing

I: ok and do you know what they do with the information that you put in as a search

R: no, what do they do with it

I: They keep it

R: I know that there's definitely something with it because do you remember very early in the new year here there was a list of the most popular searches that had been and that yeah

I: if, I tell you actually do you have a gmail account as well

R: yeah, are you going to tell me to close it (laughs)

I: no, if you go onto google and look up the google dashboard it probably is important for privacy reasons that you can see all the information they have on you on their different websites and you can clear history, I'm not sure hw effective it is but I had a look around it myself the other day and it was very interesting

R: I must have a look

I: The next bit then is about what we call resistance to surveillance, we kind of talked about it a little bit with regards to like em people filming the police filming them if they're on a protest, have you ever refused to give information to a website or a company or a government agency because you thought I don't want them knowing that about me

R: Yes my TV licence and the property tax, and not only that but I have already registered twice for the property tax once as can't pay wont pay and another time as Leon Trotsky (laughs) just because I was trying to get information from the website itself

I: that kind of answers my next question, have you ever knowingly given false or misleading information to a company, website or a government agency, have you ever asked a company or agency or anything like that to remove you from their records? or even to show what information they have about you

R: I don't know I don't think so

I: would you know how to do that if you wanted to

R: no, I haven't, or have I think I may have but I can't remember if I have or not or what exactly it was

I: say if you went home after being here today and in a weeks time this hotel started to send you loads of spam, at some stage you had told somebody here your name and address, and you knew that there was a record of you here that was being used to send you all the junk, would you know how to get off the records here

R: Well I know that there is the Data protection act that you can use because I am subject to it myself with the household charge because I am in charge of the database in Wexford and have been asked for the database by two politicians who want to send emails to the people about the household charges but now I can't I told them I can't do that you know, now of course there would be ehm I'm kind of veering away from the question again but there was a suggestion that do you know the septic tank registration, there was a suggestion that if you're septic tank wasn't adequate which I would assume they would ensure it wasn't adequate to bring in more money that that database would be sold to the companies that would be trying to fix your septic tank.

I: mm

R: I'm not sure how you would go about stopping it but there is a data protection act there

I: and when you're saying that you wouldn't hand over the database information is that because information gathered for one purpose can't be used for another have you ever heard that phrase

R: I have heard that before, and it was quoted to me at our eh national steering committee

I: ok em right so you've talked a little bit about your work as well, that you work in the hospital

R: that's only to fund my revolutionary activities (laughs)

I: how do you feel about being watched in work

R: em well I was used to be the shop steward there and there was, there was a couple of incidences where people were identified as not doing something at a particular time, and I had to clear up with the hospital management that those cameras were not for employee surveillance because that was in our rule book down there you know

I: and how did they react to that

R: they accepted it that there was nothing they could do about it, they said no you're right

I: ok and you were saying that you use the video cameras yourself

R: I have used them myself yeah I've been at the desk a few times zooming in on various people that use the hospital that we would be suspicious that they might leave the hospital, that they mightn't be in a fit state to leave you know, or somebody that eh there is often heroin users in, unfortunately that's a growing trend that, people who self harm

I: because you're responsible for them

R: if somebody comes in that's after taking an overdose the night before and is fit enough to walk up the corridor to the toilet well you do have to keep an eye on them, now there is no cameras in the toilet obviously but you'd keep the camera on the door until they come back out, and it would happen that sometimes they would be in there trying to do something and we would have to go in and open the door physically with a coin or something to open the lock to get inside

I: and is there with the work you do because there's a couple of people I've spoken to about it and they were saying that with video cameras in their workplace or even with GPS that is or isn't used with drivers that they were able to, like there was one guy who had worked in a bar and a customer had come in and given him an awful time and eventually had to kick him out, but yer man came back and complained, but to cut a long story short he said this fella had been violent, and he was able to back his story up with the CCTV footage has anything like that ever happened or have you ever seen a benefit like that of CCTV

R: yes, something like that did happen we had two people argue about something in work one day and one person made an argument exactly like that that one had been intimidating towards the other that he had stood right there screaming at them, and yes it did get caught on camera that the guy was over here still screaming at him but he wasn't standing over him in an intimidating manner but yes that has happened yes.

I: and then kind of moving away a bit from cameras what about performance objectives do you have anything like that in your work

R: no the reason being that I work as a porter and we do security as well, we only get called when we're needed and there is a reason for us, like there are times when you could be sitting down for an hour just waiting for the call to come but there wouldn't be a performance based thing

I: ok and what about if you found out that your employer was watching you outside of work like through facebook or something or keeping an eye on you outside of work

R: well I know that they do because the I was eh I was involved in I don't know if you remember the big protest about the hospital

I: I do yeah

R: I organised that and the hospital management em brought me in a couple of times about stuff that I had said to the media and the were threatening disciplinary action at one stage

I: and what kind of stuff was it

R: I had said at one stage that patients were being herded in behind the shop area like cattle and I was shown the HSE's not code of conduct I can't remember it about dealing with the media and so I had to say well I was doing that outside of work eh as a private

individual and a political activist and I challenged them to take it further but they didn't they never did. But I know that on the morning the people newspaper comes out the general managers assistant sits in her office and goes through the local papers page by page to see if there is any thing in it in relation to the hospital, not specifically in relation to me but anything to do with the hospital in it

I: and how do you feel about

R: I don't feel good about that, is the answer to that question but I would challenge it head on every time if I were to meet it

I: and how ould you feel if you were asked to complete a drug or alcohol test in work

R: again that has happened where somebody was asked to produce an alcohol test and refused to do it, now that person actually went on to go home and hung themselves. That was a bit of an issue in the hospital at the time, there was a major problem with some of my colleagues drinking on duty, you know, I don't know what it is but there's a number of alcoholics that seem to attracted to that job you know you're working late at night and I dunno what has attracted them to it, it stopped because of these issues when I was shop steward down there I laid a bit of a campaign to get rid of it because it reflected on everybody you know that there was four or five guys that were using it like a private pub up there, like stashing bottles of vodka in suspended ceilings of the private changing room you know. We eradicated that you know but .... I would be very wary of anybody being asked to provide a drug or alcohol sample by an employer

I: and why would you

R: because it's infringing on their personal rights, now if it was something that they had done at work yeah there's an argument for it, it would be a difficult thing and while I was shop steward I thought it was the most difficult thing to defend is being under the influence of alcohol or drugs at work and I told the guys and the women it's the one thing I won't go into the office over, you know my feelings and I won't be defending you

I: as a shop steward what would you think if say I was working as a porter with you and em someone in the hospital said I want you to give a sample of blood because I think you're under the influence of drugs and I said no

R: I would defend you then

I: and what would you think the assumption is
R: I would be asking I would take you out of the loop first of all and I would be asking the person whoever asked you why they would assume you were or what would there logic be for asking you to do it, now they can do it, they are entitled to do it we've been told, I've never seen it done in the hospital except for the one time the guy was asked and he refused and later that night committed suicide, he was under the influence of alcohol that day and he would have been sacked because it wouldn't have been his first time being drunk you know but it is a difficult one and ... I would have major problems defending someone who was under the influence of you know it it would put somebody in a very difficult position to defend it but if I though you weren't under the influence myself I would certainly defend you if I thought you weren't in the wrong. If I thought you had had a pint at your lunch break I probably would defend you as well, if you were falling around over patients and putting patients in danger then I think I'd probably hang you out to dry ya know
I: and what about CCTV then in general public places, do you think they work or what are they for
R: they do work em because they were used in that case where a girl was run over on the street by the guy, he came down a one way street and mounted the footpath and hit her, but they do work. With the public they are largely unseen you know the people they forget about them you know, they're not use ti being watched so they are largely in the background, I feel uncomfortable when I know that its, it's like somebody sticks a video camera in your face at a wedding you know and you go all quiet you know but.
I: and do you think that somebody is actually watching them or
R: I would say no there's nobody watching them but they're probably recording so that it can be watched so if there is an incident they can be watched and it can be played back like the system we have
I: ok you said earlier that you thought some of your internet stuff was being looked at and you used an example from years ago of someone looking at your house, has the fact that you thought you were being watched ever changed your behaviour
R: no, no it hasn't because I don't think there's anything, I fully believe in what I'm doing so if there is somebody watching me it's not going to stop me from being

politically active you know, if they, if I see them do it of course it's going to make me feel uncomfortable but it's not going to make me change my plans for the day just because these guys are looking across the road at me or whatever and that was only a couple of times that I thought that was going on and it may not have been em I am very sure that people would in some cases like we mentioned terrorism I'm sure if you thought you were being watched you're not going to go planting bombs or anything but if you're just politically active and making protests against say the current government and that in a non violent way then I've nothing to hide so (laughs) come along and join the protest,

I: Vignette 1

R: well you know it depends on how they are going to use the information, if he was within the law, I don't think his privacy was like I mean the number of his car is already going to be on public record in the registration office or whatever and eh what else did you say the direction and the time, where he is going at a particular time I mean it's indeterminate what his destination was so if he is only passing by on the Wexford road and maybe he is going to Rosslare, maybe Enniscorthy it's hard to tell so I don't think that's

I: What would you think if an organisation like the Guards was able using speed cameras that it kept records that they weren't focused on an individual but they automatically compiled people and places at a particular time and that these were searchable at a later date so if you were in a Garda station a month later they would be able to tell you places your car has been over the last few months what you think of that

R: again I would feel that is an invasion of their privacy on the one hand and I'm sure that on the other hand you could argue that if something had happened on that road and they were being used as a witness or a possible witness for something that had happened then there's positives in it as well, I definitely think it would have to be closely controlled, how wide the scope for using the information would be important, yeah it's a tricky enough question that yeah I would say I would be hesitant on them using the information really

I: ok Vignette 2

R: No and that's something that really annoys me about the internet you know I bought tickets to go on holiday to Spain to go to Barcelona for a weekend, and every time I go on you tube now here's Barcelona, and it's taken me ages to actually notice that, that there is stuff being advertised to me that I'm directly interested in

I: and where do you think that information comes from

R: Obviously it comes from Google, you tube is a google site so it's obviously them but its only recently I've made the connection that there's my Barcelona trip there you know. and this thing about using it for marketing that really annoys me, because of this campaign that we are going for the household charge, I wanted to compile a list of numbers that I could just with one click send out a message, so yesterday I went onto somebody told it's called clikitel you can buy credit on it and just send it out with one click. They were looking for very little information to get on the site but then they were looking for you had to click and tick boxes not to have certain tool bars and all installed on your computer and that really bugs me

I: That's referred to as the default setting which is privacy by choice, and the other way is privacy by design so that is something that many people are annoyed about you're not alone

R: But I find that you have to, you have to make the effort to maintain your privacy there rather than them giving you a much clearer option because normally the option id just next next next next and then install like babylon is one I saw on someones computer there, it was on mine for ages and ot took an awful lot of effort to get it off but eh merely deleting it from the programs didn't get rid of it you know, and I do find this type of thing you know that if you go into one site that they use your information to track where you're going

I: do you know any ways to counteract that

R: eh no other than to lie (laughs)

I: that's what alot of people do there is EU legislation the right to be forgotten

Vignette 3

R: well I find that unacceptable as well but I do use a tesco card it's not mine it goes onto my mothers card, I don't have one myself, this I would say has alot to do more with globalisation than anything else about selling more products to tesco customers and it is

something that worries me that you have much more, I mean you don't get that at the local shop on the corner or the shop down the street you know and it allows these big stores to wipe out smaller competition now you know 'cos they're able to profile these customers to decide what they want, you know even what they want to see when they come through the doors just by what they're buying

## Appendix 4: Garda Response to Request for Information re ANPR

Kenny

Further your email of the 7th March 2013; An Garda Síochána will not be in a position to make a reply to your questions. For information publicly available on 'Automatic Number Plate Recognition' (ANPR) - you should go onto the Garda Website, www.garda.ie under traffic tab, click on 'New Technology' this will bring up information on ANPR.

Disclosure of Garda operational information will only be in a way that is compatible with the purpose for which the information is collected for, and with the consent only of the Garda Commissioner. Under the Data Protection Act 1988-2003 the Garda Commissioner is the Data Controller and has ultimate responsibility for oversight with respect to information capture, retention, and access.

If you have any questions, you can contact me at below.

Regards

xxxxxx

Garda Research Unit

Templemore

## Appendix 5: Tesco Response to Request for Information re Clubcard Data

Dear Kenny

Thank you for taking the time to contact us with your interest in how we collate and use our data.

I'm afraid that information is confidential for business security purposes, which I hope you will understand.

Once again, thank you for your time and I'm sorry that I couldn't be more specific.

Kind regards

xxxx
Clubcard Customer Services