# 13 Surveillance Privacy and Technology: Contemporary Irish Perspectives

## Kenny Doyle[1]

## Abstract

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. 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. Using Harper's (2011) typology of subject positions, a further aim was to uncover any discursive repertoires used when defining or speaking about these concepts. It was found that widely used conceptions of privacy and surveillance are inadequate to describe contemporary reality; and that forms of sociality have changed with the widespread use of information and communication technologies (ICT).

**Keywords: surveillance, technology, privacy, Ireland, dataveillance the internet, social networking, ICT.**

1. Waterford Institute of Technology, Waterford, Ireland; kdoyle@wit.ie

## 1.     Introduction

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 (2008) 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" (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).

Since then 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. The question to be asked however 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 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 of digital technologies which are characterised by the fact that they leave information in their wake. 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 chapter 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.

## 1.1.    Surveillance

Surveillance is defined in the Oxford English Dictionary (2012) as "close observation, especially of a suspected spy or criminal" (p. 734). This definition is typical of the embodied and ocular definition of surveillance; it describes the physical act of a 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 who would most likely be the focus of surveillance: 'a suspected spy or criminal'. In common parlance, surveillance is a value laden term with which there is an implicit association of 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 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. Yet even with these examples, a vast and ever increasing field of surveillance is still excluded; 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 (CSO) reported that 78% of all Irish households had access to the internet, up from 57% in 2007 (CSO, 2011, p. 5). The take up of internet enabled smart phones is predicted to increase (Amárach Research, 2011) and the use of social networking is estimated at around 68% of the population (Comscore, 2011; Ipsos Mrbi, 2012). As well as telecommunications and the internet, there are also a number of other processes which are prevalent, such as 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 data subjects. This form of monitoring of digital remnants is referred to as dataveillance by Clarke (1988). Dataveillance – which is shorthand for data surveillance – is described as the "systematic monitoring of people's actions or communications through the application of information technology" (Clarke, 1988, p. 499).

While commonly held conceptions of surveillance most often relate to the physical watching of embodied individuals in space and time, dataveillance is concerned with recording the traces people leave behind as they go about their daily lives. The permeation of information and communications technology into almost all spheres of contemporary life means that people are constantly and unwittingly leaving digital markers in their wake. Whether it's through the use of mobile telephones, the internet, credit or debit cards, customer loyalty cards, or even simply driving on a public road past speed cameras, data is constantly being generated. This data is used by an array of state, corporate and commercial actors to identify, profile and classify whole populations. The reasons for doing this range from customer relations management, law enforcement, to consumer profiling for the purpose of direct marketing.

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 devised by Lyon (2007). He defines surveillance as "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' refer to the observable actions just as much as the digital traces left behind, as well as the extension of the reasons for surveillance beyond the implicit suspicion definition offered above.

## 1.2. The Panopticon

While the most common metaphor used in common parlance when talking about surveillance is Orwell's (1948) *Big Brother*; the ubiquitous metaphor in

surveillance studies literature is the Panopticon. This was a model for a prison originally envisaged by Utilitarian philosopher Bentham (1787/1995) who saw 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" (p. 29).

The idea for the Panopticon was elaborated in a series of letters written by Bentham in 1787. He saw it as being more than an efficient means of operating institutions and claimed that it could be used as part of a viable plan for widespread social and disciplinary reform. 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 backlit, which makes them and their occupants constantly visible to the inhabitant of the inspection tower. The key however is that the inspector is invisible to those in the cells and thus power is tied in with visibility. The gaze from the inspection tower is unverifiable and so the inmates must assume that they are under constant observation and behave according to the prescribed norms of the institution. Bentham (1787/1995) did not see this as being just a means of controlling inmates or maintaining order inside institutions. He saw it as being a "new mode of obtaining power over mind, in a quantity hitherto without example" (Bentham, 1787/1995, p. 30). This 'power over mind' would allow for effective rehabilitation of inmates and would act as a mode of re-socialisation, where errant ways of being could be corrected through constant surveillance, with the aim of keeping inmates close to prescribed norms of behaviour. 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 does not try to do so. Instead the purpose 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 tend to 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).

Foucault (1977) used the idea of the Panopticon to underpin his schematisation of the Disciplinary Society. Foucault (1977) saw the Panopticon as being emblematic of a new form of discipline, a new mode of exercising power which was productive rather than destructive. 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 power and violence, 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 Panopticon is a central metaphor in surveillance studies; technologies such as the video camera may have rendered the architectural design redundant; yet the underlying idea of imposing discipline through potentially constant yet unverifiable monitoring has endured. Poster (1996) extended the panoptic metaphor to include the capability of technology to facilitate the digital 'super-panopticon' and Lyon (1994) has described the 'electronic Panopticon'. The technological removal of spatial and temporal limitations allows for the spread of panopticism beyond the bricks and mortar of the inspection tower envisaged by Bentham (1787/1995). In its original guise, panoptic power was exercised by a central authority as a means of enforcing institutional norms. The main argument against the different forms of digital Panopticon is that there is no central authority which has the requisite power to rule over a dispersed, decentred and supra-national network such as the internet.

Mathieson (1997) noted the operation in concert with panoptic methods and practices of 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" (p. 219).

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 this 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. 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. Where panopticism operates through coercion, or at least the threat of coercion, synopticism operates through seduction or inducement towards particular culturally desirable behaviour. 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 taught what the norms are. If the Panopticon relates to the invisible watching of power, then the Synopticon relates to the broadcasting of power. 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.

By way of example, Andrejevic (2004) claimed that reality television programs acted "neatly as an advertisement for the benefits of submission to comprehensive surveillance" (p. 2). Reality Television shows such as *Big Brother* or *Survivor* operated according to two main principles: firstly that contestants were drawn from the public at large and secondly that fame and fortune were possible through the process of opening oneself up completely by being constantly on display. Surveillance is thus seen as a key facilitator of reality as it forces participants to be their true selves by making it difficult to maintain a false front. At the same time, such shows valued self disclosure and self expression above all

else. Reality television programs synoptically normalised such a culture of self display as a means of attaining wealth and status, and in the process normalised systems of surveillance:

> "Pervasive surveillance is presented as one of the hip attributes of the contemporary world […]. In this respect the reality trend aligns itself with the efforts of the proponents of the new economy to destigmatize surveillance and reposition it as a form of convenience" (Andrejevic, 2004, p. 105).

This repositioning of surveillance ties in with the advent of a widespread culture of display. The motivations and attitudes identified by Andrejevic (2004) while describing reality television have since diffused across society via social networking and other forms of networked communications. These motivations include the wish for users to be visible and available which may seem at first glance to be anathema to commonly held and traditional conceptions of privacy.

## 1.3. Privacy

To define privacy is a notoriously difficult task; the Oxford English Dictionary (2012) describes it as "a state in which one is not observed or disturbed by other people, the state of being free from public attention" (p. 572). This definition is overly individualistic and describes just one aspect of privacy, namely seclusion. In these terms privacy is essentially formulated as Warren and Brandeis's (1890) "right to be left alone" (p. 194). 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. Here privacy would be lost as soon as one enters social relations, as the perfect state of privacy is isolation. In this sense privacy is also commonly described in terms of a spatial metaphor, where its violation is spoken of as an invasion. A more complete definition would include reference to privacy involving the ability to control to some degree the dissemination of information regarding one self. This element can be found in the definition of Westin (1967) who states that privacy is "the claim of individuals, groups,

or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7).

In his study of the interaction order of social life, Goffman (1959) devised a scheme based around the dramaturgical metaphor. This scheme viewed social life in terms of performances, where people present themselves in particular ways depending on the situation. The dramaturgical metaphor was utilised when describing front and back areas. Front areas 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 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. A Goffmanian perspective on privacy 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. Jenkins (2004) 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" (p. 71). 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. At the level of the individual, Westin (1967) claims that this ability to withdraw to the realm of the private facilitates reflective solitude, allowing 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" (cited in Steeves 2009, p. 198). This reflective solitude also allows for intellectual development and for the undertaking of complex tasks, free from the interruption of others, which benefits both the individual and society.

These definitions of privacy are 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 need for a social perspective on privacy is succinctly stated by

Moore (1984) who claims that "the need for privacy is a socially created need, without society there would be no need for privacy" (p. 73). In the back areas mentioned above, not only is there a 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 (1967) defined the fullest state of privacy in terms of withdrawal from sociality; Altman (1975) defined privacy as "a dynamic process involving selective control over a self-boundary" (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, 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 and intimacies earned and maintained.

Despite the benefits granted by privacy to individuals and society, there is growing credence given to the idea that increased transparency is both desirable and necessary. As we have seen above, the desirability of transparency has been strengthened by norms set synoptically by reality television and celebrity culture. The necessity for transparency however is often couched in terms of security, where the rationale for any new surveillance measure is most often to prevent crime: criminal 'others' commit crimes and so these people that are the intended targets of surveillance measures. Such measures should thus not concern those who abide by the law and have nothing to hide.

## 1.4.    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 (2008) claims that this phrase is inaccurate because it fails to adequately account for the full definition of privacy, and sees it just as being about 'hiding a wrong' (p. 79). Privacy in these terms is seen as a screen behind which illegal or immoral deeds can be obscured. As we have seen above, 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 (2006) 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" (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.

## 2. Methods

Surveillance and privacy are topics that have been and will continue to be widely researched across a range of disciplines. The most wide reaching research is the Globalisation of Personal Data (GPD) Project International Survey on Privacy and Surveillance[1] conducted in 2006/2007 at Queens

---

1. Retrieved from https://qspace.library.queensu.ca/bitstream/1974/7659/23/GPD_Survey_Methdology_2011-11-13.pdf

University Toronto. In the European context, Eurobarometer polls 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. 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.

## 2.1.    Context and participants

This study was conducted between September 2010 and April 2011. The aim of the study was to ascertain the knowledge levels of Irish citizens with regard to digital surveillance and its effect on privacy, to understand how these concepts are defined, and how people interact with these systems by aiming to uncover any discursive repertoires used. A further aim was to explore how practices of surveillance are instituted in differing social situations such as contemporary work, consumption and law enforcement. The study aimed to get a bottom up view of surveillance by investigating the lived experience of those who are subjected to it. In order to get such data from interview subjects, it is preferable to allow them to speak in 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. Therefore, the qualitative interview was the method employed in this study. The open ended nature of qualitative questioning allows for the expression of the participants' understanding, knowledge, experience and values in a meaningful way. Bryman (2008) 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" (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, participants generated areas of interest not foreseen by the researcher and were able to express the elements of the field which were of importance to them and thus worthy of further questioning. With each participant, the location of the interview was designated as a place of their choosing, either in the participants' home or in a neutral location such as a hotel, coffee shop or pub. The only stipulation was that the location be quiet enough to allow for the recording of decipherable audio. The style of the interview was determinedly informal, every effort being made to make the subjects at ease and comfortable. The interview followed a semi-structured template, with a list of topics and questions to be covered but the order in which they were discussed 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 analyse them at a later stage.

The sample 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 respondent was nineteen years old, and the oldest was forty-six. As per the instructions of the ethics committee of Waterford Institute of Technology, there were no respondents under the age of eighteen. There were varied methods of recruitment; the first phase involved simple word of mouth where acquaintances and friends were asked to nominate people known to them but not to the researcher, this yielded a total of five interviews. At each interview respondents were asked if they would nominate any other people, this method of snowballing yielded a further four interviews. At this point the age profile was in the high thirties and a concerted effort was made to find participants between the ages of eighteen and twenty-five. The remaining six respondents were recruited through a group page set up on *Facebook* which

outlined the details of the project and asked for interested people to get in touch. This method allowed for a greater geographical spread with interviewees from a broader range of locations in Ireland. The use of social networking as a tool of recruitment allowed for the targeting of people within a specific age range; however, it only allowed for people who used social networking sites to take part, which meant that the eighteen to twenty-five year old demographic who do not use social networking sites was not represented.

## 2.2. 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. Such variance of meaning does not always allow to determine which sense of the word the interviewee is using. A means of addressing these problems was through the use of content specific vignettes: this method involved the construction of brief third person narratives as examples of the concepts in question. In drawing up the vignettes to be used, a number of factors had to be considered. Stories must be believable, describe everyday situations, and avoid exceptional situations, circumstances or characters. In using content specific vignettes, the aim was to describe mundane, believable and relatable situations and characters (Barter & Renold, 1999; Finch, 1987; Veal, 2002). A further element of consideration was the length and complexity of the vignette; Finch (1987) claims that more than three changes to a storyline in a vignette will render it too complex and difficult for respondents to remember (p. 107). The vignettes used were thus short, concise and to the point: there were scarce details given which would influence or lead the respondent. An example of one vignette was:

> *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. This information is used by the supermarket to tailor special offers and discounts to Ann.*

After the vignette was read, the respondents' opinion was sought about potential issues raised by asking an open question such as "what do you think about this?" 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 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.

# 3.    Results and discussion

## 3.1.    Defining terms

During the interviews respondents were asked early on to define both surveillance and privacy. Overall the definitions of surveillance matched the embodied ocular definition as typified by the dictionary definition given above. The most commonly mentioned form of surveillance was CCTV; yet when they were gently pushed towards talking about data trails, all respondents knew something and were able to speak at length. Most respondents also defined surveillance in negative terms, as being the exercise of malevolent power which was imposed on people, yet others mentioned situations where surveillance operated in their favour. One person noted how financial institutions monitor transactions so as to minimise the occurrence of fraud:

> **Mark:** I know like that the bank like would kinda use transaction history… I mean I was on holiday before and they'd actually like you'd get a phone call because you're in a foreign country spending… because they don't know whether it's you or not and the history might suggest that you're not going to be abroad spending that kind of money… so they are kind of I suppose they are keeping an eye on you really.

An addition to Lyon's (2007) definition of surveillance was given by Peter, aged 45, who was quite knowledgeable about elements of internet monitoring yet weighed these factors up against the convenience offered by the technology, "at the end of the day it makes life easier". This same logic of convenience was also applied to internet shopping for groceries,

> **Peter:** I know they keep all of your details like a record of what you eat and stuff but ya know like it's better than being stuck in a supermarket on your day off with lots of screaming kids.

So despite Peter being quite knowledgeable about consumer profiling, the short term benefit of convenience outweighed the more abstract and merely potential costs of surveillance and profiling. Lester (2001) talks about the "tyranny of convenience" which describes how "consumers are compelled to go online for an increasing array of transactions" (p. 28, cited in Andrejevic, 2002, p. 238). The methods of compelling consumers online are usually based on considerations of cost efficiency or convenience, so in Peter's case it was the convenience of being able to shop quickly from home that informed his choice. A further example of incentivised migration to online service can be seen in banking, where customers are offered reduced transaction fees on the condition that they activate and use an internet banking service. A further question asked if respondents would be happy to give up personal details or elements of their privacy for financial gain and almost all replied in the negative. Interestingly however, one of the vignettes described a situation involving a supermarket customer loyalty card and many of those who answered in the negative actually used these cards.

In defining privacy the majority of respondents mentioned both the spatial metaphor and Westin's (1967) notion of controlling information flows regarding themselves (p. 7). In discussing the control of personal data flows, there were common references made to particular privileged data such as financial details and health records. Privacy was thus described as a bulwark against identity theft which is believed to be prevalent although no respondent knew personally of any instances of its occurrence. The spatial metaphor was

commonly described in terms of the home being a privileged space which falls under the control of its occupants. The socially contextual nature of privacy was also often mentioned:

> **Hannah:** I think people have different levels of privacy, some people find stuff that maybe that I would have no bother sharing with people.

This quote illustrates the variation of privacy expectations; as noted above, the popular distinction between private and public is oversimplified. What is seen as private will depend upon a multitude of factors such as culture, personal opinion or social context. The contextual nature of privacy as previously described by Nissenbaum (2010) and Zimmer (2008) is not just dependent on the situation; Hannah defines privacy as a subjective value which also differs according to who is making the claim.

All respondents believed that we now have less privacy than we did in the past, and all bar one blamed technologically mediated communication for this.

> **Sean:** It's very obvious that we have less because we're depending on much more artificial means of communication as well, we're not communicating as much face to face as we were you know.

Only one respondent spoke of privacy as being socially beneficial, all other definitions spoke of it in terms of an individual good. The social benefit mentioned was that privacy allowed for and even fostered creativity, in response to the question what would you think would happen if privacy was completely lost this interviewee said:

> **Rory:** Em I think you would get a society that would totally lack creativity, it would totally lack any form of innovation in themselves because I think that no matter what they do, what they create any idea they have is gonna be taken, taken from them, …I think it comes down to every sort of innovation or any sort of creativity that people have or any sort of idea it would just totally stifle creativity and progress.

Rory equates privacy with creativity which is a sentiment seen above in Westin's (1967) concept of reflective solitude, which allows people the space to experiment and try new ways of doing things free from the view of others. Reflective solitude allows for intellectual development and for the undertaking of complex tasks free from interruption. Innovation and creativity are thus coupled with privacy in the form of reflective solitude. The strict monitoring of tasks leads to employees matching their work to the standards they believe to be expected of them in what Zuboff (1988) calls 'anticipatory conformity'. This is similar to the exercise of panoptic supervision, where workers act as if the eyes of their supervisors are on them at all times and behave in a manner which they anticipate will conform to their expectations. This leads to risk averse behaviour where employees will not act outside of given guidelines and this "would severely curtail creative thinking, as employees would begin to act and then think in response to an unseen observer" (Martin & Freeman, 2003, p. 356).

## 3.2.    Discursive repertoires

Harper (2011) denotes three broad subject positions when speaking about surveillance: the suspicious position, the indifferent position, and the position of balancing (p. 2). All three of these repertoires among others were evident during the interviews. The suspicious subject position is often correlated to discourses of paranoia, "this term appears to be deployed to undermine the legitimacy of a suspicious position as we see when more suspicious narratives are denoted as conspiracy theories" (Harper, 2011, p. 2). Thus when respondents characterised themselves as suspicious of surveillance they often felt the need to distance themselves from being perceived as being paranoid or from being believers of conspiracy theories. This was evident for example when Anna a 27 year old said:

> **Anna:** We are a technological society, all that information, I don't think you're even aware of how much your information goes you know you join all these different sites and God knows who knows what, and there could be some big guy in this big building just you know accumulating it all into graphs, to make a few bob you know, although that's a bit of a conspiracy theory I try not to go there (laughs).

There are a number of interesting points in this section; firstly Anna is describing the process of information capitalism (Wall, 2006, p. 340), where personal data is garnered, warehoused, interrogated and ultimately mined for the purposes of extracting useful information for sales and marketing. The internet adage originally espoused by the blogger Andrew Lewis (2010): "if something is for free then you are the product" applies here; many free services online require some level of registration. As the registered service is used, it generates saleable data pertaining to the user. In social media for example, a user is required to register. As the site is used, all information is stored, aggregated and offered in some form to sales and marketing professionals. And yet, describing the process makes Anna feel overly paranoid, and makes her partially recant by saying "that's a bit of a conspiracy theory I try not to go there". Harper (2011) refers to this type of action as 'rhetorical inoculation' where the expression of views which could be labelled as paranoid is followed by laughter, joking or some method of semantic distantiation (p. 11). Another interesting point here is the anthropomorphosis of the process; in this description, it is not a computer program but "a big guy in a big building". In the same interview, Anna talks about shopping on line and mentions how she particularly loves Amazon because "they get me". This humanising of technology also came up in other interviews, in particular when talking about privacy. A number of interviewees only had a problem with dataveillance if they thought that a person at the other end was reading the content, and had no problem with the process when it was carried out automatically by a computer program or algorithm.

A further position which is related to suspicion is function creep or the slippery slope argument; this subject position states that if we allow surveillance for one reason, it will inevitably be used for many others and so the allowances made for what Agamben (2005) calls 'the state of exception' should be minimal. A central point is an ingrained cynicism, a belief that governments and state actors will opportunistically prey on public fears such as terrorism or organised crime and use them to institute surveillance measures which will increase their power at the cost of the citizenry. This argument was put forward on a number of occasions,

> **Richard:** 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, (pause) I mean there's no evidence there that it works.

Respondents were asked if they would be prepared to give up some of their personal data to the authorities if they were told it could make the country safer and it often led to similar answers:

> **Pat:** I would not believe their explanation quite simply I would, I would expect to see a lot of statistics proof and studies done that me handing, eh essentially signing away some of my privacy would actually be effective in what they claim they're trying to do I would not take their word for it.

The third and final subject position of Harper's (2011) typology is the balancing or trading off position. Sets of given dualisms, for example liberty/security, surveillance/privacy, ideally need to be balanced so as to get the best of both, such as allowing the most liberty without sacrificing security. This metaphor of balance is most commonly used in public and political discourse, and implies a certain level of rationality and reason in its proponents. People who 'balance' see themselves as active and having control over their data and privacy. This was typified by Darren:

> **Darren:** In order to get some things done you have to give up a little bit of your privacy, give away a bit of your privacy, for your own selfish kind of goals, for you to buy something or to get something you have to kind of deliver to them your bit of information, so it's a two way thing really. If you want to be paranoid and kind of worry too much about your privacy then you're not gonna get anything yourself.

Here the onus is on the individual; at a later stage in the interview, when talking about privacy, Darren states that even online, other people only have as much access to his details as he allows – in a definition which has echoes of self-governance and the responsibilisation element of the Risk Society thesis

proffered by Beck (1992) and Ericson and Haggerty (1997). In the sense of his self identity as a rational consumer, each instance of accepting a service or product is in his mind a choice, a weighing up of costs versus benefits which he should be able to assess accurately. Darren's statement is similar to what Zimmer (2008) describes as the "faustian bargain of technology" (p. 111) where benefits of technological advances must be tempered with the fact that these benefits come at a price, as Darren states "it's a two way thing". The problem with this however is that of information and power asymmetry. It is highly unlikely that in all instances of data gathering, Darren knows that it's happening, the identity of the person or organisation gathering the data, or the ultimate destination of this data. In this case it is not possible to strike a meaningful balance or make a truly informed decision.

A smaller number of respondents were quite indifferent to surveillance and saw it as something which worked in their favour. In these cases, there was common recourse to the phrase "I've got nothing to hide" (see above) and increasing levels of transparency were seen as positive and desirable aspects of modern life which could be used to hold others to account. Patrick noted how he actively sought a GPS tracker on his van from his employers so he could prove he was working at all times.

> **Patrick:** 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… 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.

Surveillance is used for Patrick to claim his entitlements, to prove he was operating within the terms of his employment and to hold his employers to account. Not being monitored had in this case tangible disadvantages for him. This position was echoed by Hannah who worked in a call centre where all

calls are recorded; every week a call is picked at random and reviewed by her manager. Instead of feeling constantly under potential supervision and feeling in a panoptical sense the need for self correction, Hannah spoke of how she found it reassuring to know that if a dispute ever arose, she would have a recording to fall back on and as such welcomed the recording of her working life.

The phrase 'I've nothing to hide' recurred across the interviews with such frequency as to warrant calling it a default position. While this view has been explored in detail above, it is worthwhile to further examine the ramifications of such a widely held belief. 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 approaching the status 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? 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' 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.

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:

> **Sean:** 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.

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 (2001) refers to as "networked individualism" (p. 129). Using the internet and particularly social networking sites as material supports for networked individualism, respondents build what Castells (2001) calls "portfolios of sociability" (p. 132) where multiple but weaker ties are created and maintained, centred 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:

> **Peter:** 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.

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 from the constraints of geographical location with people from all over the world. Locally based peer groups use technologically mediated means of communicating, even when there is no significant geographical divide. As we have seen 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.

## 4.      Conclusion

One of the more striking findings of this study is the changing nature of privacy which is best exemplified by Bauman (2010):

> "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" (p. 31).

Bauman (2010) 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 of privacy for classical thinkers was very much to do with deprivation rather than voluntary withdrawal" (O'Hara & Shadbolt, 2008, p. 21). Privacy in this sense was the domestic realm, where very little happened, as opposed to public realm of the polis where all governance, trade, commerce and public discussion occurred. Networked communications 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 Bauman (2010) rewrites Descartes proof of existing 'I think therefore I am' to "I am seen, therefore I am" (p. 20). As shown above, users of social media often see it as being more than 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. As has been shown above, 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. Moreover, these processes 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.

As communication is becoming technologically mediated; there are questions about levels of surveillance built into these 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. 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 which have normalised practices of transparency and display.

# References

Agamben, G. (2005). *State of Exception* (Translated by Kevin Attell). Chicago: The University of Chicago Press.

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. (2002). The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure. *Critical Studies in Media Communication, 19*(2), 230-248. doi: 10.1080/07393180216561

Andrejevic, M. (2004). *Reality TV: The Work of Being Watched*. New York: Rowman & Littlefield Publishers.

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

Bauman, Z. (2010). *44 Letters from the Liquid Modern World*. Cambridge: Polity.

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage Publications.

Bentham, J. (1787/1995). *The Panopticon Writings* (Edited and introduced by Miran Božovič). Ann Arbor: Verso.

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

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 Publishers.

Clarke, R. A. (1988). Information Technology and Dataveillance. *Communications of the ACM, 31*(5), 498-512. Retrieved from www.cse.unsw.edu.au/~se4921/PDF/CACM/p498-clarke.pdf

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

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

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

Finch, J. (1987). The Vignette Technique in Survey Research. *Sociology, 21*(1), 105-114. doi: 10.1177/0038038587021001008

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

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Edinburgh: University of Edinburgh.

Harper, D. (2011). Paranoia and Public Responses to Cyber Surveillance. *Paper Presented at Cyber-Surveillance in Everyday Life May 2011 University of Toronto Canada*. Retrieved from http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Harper-Paranoia-and-public-responses.pdf

Ipsos MRBI. (2012). *Social Networking Quarterly Survey May 2012*. Retrieved from www.Ipsosmrbi.ie/social-networking-quarterly-survey-may-12.html

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

Lester. T. (2001). The reinvention of Privacy. The Atlantic Monthly, 287(3), 27-39.

Lewis, A. (2010, August 26). *User-driven discontent* [Web log post]. Retrieved from www.metafilter.com/95152/Userdriven-discontent

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Manes, S. (2000). Private Lives? Not Ours! *PC World, 18*(6), p. 312. Retrieved from http://www.pcworld.com/article/16331/article.html

Martin, K., & Freeman, R. E. (2003). Some Problems With Employee Monitoring. *Journal of Business Ethics, 43*(4), 353-361. doi: 10.1023/A:1023014112461

Mathieson, T. (1997). The Viewer Society: Michel Foucault's 'Panopticon' Revisited. *Theoretical Criminology, 1*(2), 215-234. doi: 10.1177/1362480697001002003

McNealy, S. (1999). Presentation at an event launching Sun Microsystems's Jini technology.

Moore, B. (1984). *Privacy: Studies in Social and Cultural History*. Armonk: M.E. Sharp.

Nissenbaum, H. (2010). *Privacy in Context Technology, Policy and the Integrity of Social Life*. Standford: Stanford University Press.

O'Hara, K., & Shadbolt, N. (2008). *The Spy in the Coffee Machine: The End of Privacy as We Know it*. Oxford: Oneworld Publications.

O'Hara, K., & Stevens, D. (2006). *Inequality.com: Power, Poverty and the Digital Divide*. Oxford: Oneworld Publications.

Orwell, G. (1948). *Nineteen Eighty-Four*. Retrieved from http://gutenberg.net.au/ebooks01/0100021.txt

Oxford English Dictionary. (2012). 7th edition. Oxford, England: Oxford University Press.

Poster, M. (1996). Databases as Discourse; or, Electronic Interpellations. In D. Lyon & E. Zureik (Eds.), *Computers Surveillance and Privacy* (pp. 175-192). Minneapolis: University of Minnesota Press.

Schneier, B. (2008). *Schneier on Security*. Indianapolis: Wiley Publishing.

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. London: Yale University Press.

Steeves, V. (2009). Reclaiming the Social Value of Privacy. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 191-208). Oxford: Oxford University Press.

Van Dijk, J. (2006). *The Network Society* (2nd ed.). Thousand Oaks, CA: Sage Publications.

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

Wall, D. S. (2006). Surveillant Internet Technologies and the Growth in Information Capitalism: Spams and Public Trust in the Information Society. In K. D. Haggerty & R. V. Ericson (Eds.), *The New Politics of Surveillance and Visibility* (pp. 340-362). Toronto: University of Toronto Press.

Warren, S., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. Retrieved from http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

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*. New York: Basic Books.

Research-publishing.net

Internet Research, Theory, and Practice: Perspectives from Ireland
Edited by Cathy Fowley, Claire English, and Sylvie Thouësny

The moral right of the authors has been asserted