

How does surveillance affect society?

This essay will be a critical analysis of mass global surveillance that is invading the privacy of innocent people from all around the world, (Timm, 2014) and will discuss the affects of this and where the line should be drawn between privacy and surveillance. The valuable publication, authored by Michael Seemann, *Digital Tailspin: Ten Rules for the Internet After Snowden*, will be the main focal point of reference as this paper will analyse and reflect upon several interesting and topical theories and concepts from within the rules 0,1,2, 3 and 8.

Primary research will be gleaned in order to explore exactly the effects that the “filter bubble” has on individuals in society online today. Furthermore, through taking a broad look at online discussions and journals this will benefit to further understand the affects that mass surveillance has on the entire population of the world.

There are many interesting discussions and debates, from privacy to state secrets that revolve around the problems and difficulties that Ulrich Beck calls ‘second modernity’; the risk society (Beck, 1992), or what Michael Seemann is calling *Kontrollverlust* that translates to the loss of control (Seemann, 2015).

There is a concept that Seemann puts forward in his publication, which is the *irretrievable loss of privacy* (Seemann, 2015). This is a profoundly controversial thesis. Particularly in Germany, the whole notion of privacy underlies so much of the distrust that the German state has got over any kind of surveillance. This goes back to the time when certainly in East Germany, you have the communist regime which was very much a surveillance based state. But it was not the kind of surveillance we think of now; multitudes of cameras, every mouse click being traceable – it was a different kind of surveillance based on huge numbers of the population being part of the Stasi (the European secret police).

This really created an atmosphere of paranoia, where you just didn’t know who your friends or even your family were reporting back to about your behaviour, which could in turn change everything from your career prospects to even your own fate. So that notion of a surveillance society and resistance to it is profoundly embedded in the GDR (German Democratic Republic) and a kind of fear of that has made the German population allergic to any form of state surveillance whatsoever.

Whilst some countries are completely relaxed about Snowden's revelations about mass surveillance through the NSS, in other parts of the world, particularly parts that previously had a big dominance of state surveillance are far more paranoid about that and that includes Germany. Countries vary a great deal about how much trust they're going to give their governments and this issue of trust has a profound effect on how people look at this issue of control.

The 'Black Swan' (Taleb, 2007) is used by Nassim Taleb to describe how people always try to predict and how we are now living in a world where there is radical uncertainty. He states a modern world is a world where insurance companies and all sorts of industries are all based on the idea that it is possible to not control individual risk, but be able through calculation to be able to come to very firm conclusions about levels of risk in society. But Rumsfeld's proposition of the 'Unknown Unknown's' (Graham, 2014) is the opposite; the things that nobody could ever predict have a big influence on which the way history happens, the way in which development happens and the way in which individual lives happens. On an individual level we do everything we can to predict things for ourselves, to make sure that we have all the best possible chances, but inevitably the real things that really change our lives, for better or for worse, are things that come completely out of nowhere. The more complex the world becomes and the more complex the information environment becomes the more impact unpredictability has on the way that things develop, both individually and in terms of corporations, nations and the world.

Donald Rumsfeld best describes this after 9/11 (Donald Rumsfeld Unknown Unknowns, 2007) when he talked about the 'Known Knowns'; the effects and risks that are out there that we are familiar with. The 'Known Unknowns'; the stuff that is out there that we know about, yet we do not really know the details of; We know there are certain sorts of threats, but we just have not got enough information to be able to control them and this relates to the very recent investigation of the Talk Talk hack, where a vast number of personal customer details were accessed (BBC, 2015). And the thing that he said that was most scary and most distinguished from everything else is the 'Unknown Unknowns'; the things that are out there that will come at us and that there is no way that we can know them. How can you manage

risk in a society where the number of Unknown Unknowns has accelerated? After the catastrophic events of 9/11 one might think you no longer could.

German sociologist Ulrich Bech coined the term *The Risk Society*. He made a proposition that in the first era of modernity, the Industrial Revolution, you had something which was based around calculable risk, the idea of probabilities; which is based around the fact that although your individual life chances and risk aren't calculable, if you aggregate that to large numbers then you can draw conclusions which means that risk overall is calculable (Beck, 1992). What has happened in Industrial society since is the idea that risk can ultimately be controlled by science and rationality and that this is something upon which our society has been based. What Bech suggested was that something had happened since and what he calls '*second modernity*' (*the second revolution of modern society*); when modernity starts to modernise itself and the world starts to become ever more complex and reflexive and the systems that inhabit it also become the danger as well as the solution.

Nassim Taleb states that we have moved from an era of probabilities being able to calculate risk through to an environment of radical uncertainty (Taleb, 2007), radical incalculability and unpredictability, which really changes the game. There are three drivers that Seemann claims are the driving force of this loss of control (Seemann, 2015):

1. Total surveillance
2. Infinite copying and dissemination
3. Pattern recognition

'We', the people, do not know how we are being surveilled and one may state that this is a huge issue in modern day society. The UK seems to be most comfortable with this considering it has had more cameras put in to its environment watching their citizens' every move than any other country (Weaver, 2015). There is also total surveillance of our every mouse click. Mass surveillance involves postal service surveillance, social network analysis, aerial surveillance, biometric surveillance, data mining and profiling, corporate surveillance and satellite imagery (Wsystems, 2010). There is a distinction between observation and surveillance, however, which is the level of power an observer has over its subject. It is a question of control.

Almost everything a user discovers on the Internet has been copied from somewhere else (Mirani, 2015). Whatever the content is that is created on the Internet, there is always has the chance that it will be copied, distributed and disseminated. Machine algorithms, Big Data and other modes of pattern recognition are used to manage and control these colossal amounts of data and to filter and to glean knowledge and interpretation from it.

Surveillance, however, is not necessarily all a bad thing. It does help investigations and there are tools and computer algorithms that personalise the Internet for the user and makes it easier for them to navigate around, such as the “filter bubble” (Pariser, 2011). Snowden, however, says that intelligence agencies are not all out to get everyone and that it is in the public’s interest to have some level of intelligence gathering to investigate criminals and to respond to military threats etc, “but that is a far cry from watching everyone in society without any regard to their guilt or innocence to the mass surveillance of entire populations rather than individual people and that’s something that if we decide to go in that direction, were that ever allowable or legal in the first place which I will argue it’s not, that is fundamentally a decision that the public has to make and not some official that is behind closed doors” (Live Q&A: Edward Snowden, 2015).

Without a doubt the world is a safer place with surveillance, but it is getting so out of control and rather ‘over-the-top’. To date, we have very little insight as to how these algorithms operate, what incentives are behind them, what data is used and how it’s structured. There is this question of who owns data as well? Is it us or is it ultimately GCHQ, the NSA and other organisations and agencies, which we the public do not have access to? It seems that governments want more power and control over its people. For one reason, the UK wants to ban encryption altogether (Telegraph, 2015) but as Snowden says “even with that encryption, law enforcement officials can still ask for warrants that will give them complete access to a suspect’s phone, which will include the key to the encrypted data” (Ha, 2014). There are hacking tools that the GCHQ attain that can turn mobile devices on even when they are switched off without you even realising, or turn on its GPS so that its location can be pinpointed and turn on the microphone to listen in on you (Smith, 2015). This software is known as the ‘Smurf Suite’ and the GCHQ are firmly linked with the NSA, which both share intelligence with one another (BBC, 2015).

The query is relatively a form of surveillance as well, which is the ubiquitous eye. It is watching our every move on the Internet and monitoring it and is central as a means of structuring content in the 'new game'. The way users experience content now is through asking questions and queries. This shift in how information is flowing online is invisible. There are no borders as Seemann states (Seemann, 2015) and no gatekeepers that control the flow of information that was present in the 'old game' as Pariser states also (Beware online "filter bubbles", 2011). With web companies now determined to tailor their services such as search results and news feeds to its user's personal interests through algorithmic editing, they trap us in what is so-called the "filter bubble". A filter bubble that is your own personal unique universe of information that you live in online (Beware online "filter bubbles", 2011). One may agree with Seemann's proposition about the "filter bubble" in rule three where he states "filter bubbles" will tend to preserve your own point of view, and insulate you from other opinions" (Seemann, 2015). This varies a great deal on different platforms. Facebook and Twitter's tools for example allows users to create their own "filter bubbles" by simply following or un-following other users, cherry picking what flows through your own personal news feed that is unique to the user. Again, who owns this information? Is it us, Facebook or the NSA and GCHQ? Google on the other hand puts you into a "filter bubble" automatically. Everything a user searches or clicks on, Google keeps a record of and are accumulating vast amounts of data about us without us even realising.

Experiment

As part of the primary research an experiment has been conducted to personally investigate and identify the effects that the "filter bubble" has on individual users online. Pariser mentions in a Ted Talk that two of his friends got two extremely different results when searching "Egypt" and concluded, "the Internet is showing us what it thinks we want to see, but not necessarily what we need to see" (Beware online "filter bubbles", 2011). I gave three subjects the task to generate three different queries into Google: "Syria", "Protests" and "Books" (see Appendix), all separately and see just how their searches compare from one another, if at all. This aims to put the theory to practice, which turned out to be false in my case. All the subjects got the exact same results, which completely contradicts what Seemann said about the "filter bubble" in rule three; "Google has become so highly personalised, he states, that no two people would ever get the same list of results for

the same query” (Seemann, 2015). This demonstrates when putting the theory in to practice it does not work, but maybe one way of improving this experiment is to use many more subjects and use more in-depth queries and searches.

I do, however, agree with the concept of the “filter bubble” to some extent. I agree that on Facebook, Twitter, Instagram and other platforms a user does create and configure its own “filter bubble” that may preserve one’s point of view. That being said, I do not consider the “filter bubble” as being such an immoral form of surveillance, based on the results gleaned from the experiment.

Surveillance really does affect the people it monitorises on an individual level. Speaking for myself I do self censor and refrain myself from posting certain things on a social network. I am continuously conscious of what I say, share and post because it may harm my chances of employment. There are indeed ways in which my own freedom to act and express myself is being constrained almost without me realising it. I often ask myself to what extent is my behaviour already being affected by the knowledge that I can’t control my own data body? To what extent have I already compromised my freedom without realising it? It certainly does not happen over night, but suddenly you look around and the sense we have of freedom to express ourselves are be being constrained in ways that we would not have chosen. The famous metaphor of a frog used in a myth to describe how small incremental changes can lock you into things where you suffer can be used to describe this best; If you drop a frog in water that is already boiling it jumps out, but if you gradually put up the heat it dies. One can draw parallels from this analogy that the heat is being raised and that it is only at a certain critical point that you realise just how much freedom you have given away.

Appendix:

1st query – “books”.

Link 1: <http://www.amazon.co.uk/books-used-books-textbooks/b?ie=UTF8&node=266239>

Link 2: <http://www.whsmith.co.uk/books>

Link 3: <https://www.waterstones.com/books/bestsellers>

Link 4: <http://www.theworks.co.uk/page/books>

Link 5: <https://books.google.co.uk/>

2nd query – “protests”.

Subject 1:

Link 1: <http://edition.cnn.com/2015/11/10/us/missouri-football-players-protest-presidents-resigns/>

Link 2: <http://www.theguardian.com/world/protest>

Link 3: <https://en.wikipedia.org/wiki/Protest>

Link 4: <http://www.thesaurus.com/browse/protest>

Link 5: <http://www.protest.net/>

Subject 2:

Link 1: <http://edition.cnn.com/2015/11/10/us/missouri-football-players-protest-presidents-resigns/>

Link 2: <http://www.theguardian.com/world/protest>

Link 3: <https://en.wikipedia.org/wiki/Protest>

Link 4: <http://www.thesaurus.com/browse/protest>

Link 5: <http://www.protest.net/>

Subject 3:

Link 1: <http://edition.cnn.com/2015/11/10/us/missouri-football-players-protest-presidents-resigns/>

Link 2: <http://www.theguardian.com/world/protest>

Link 3: <https://en.wikipedia.org/wiki/Protest>

Link 4: <http://www.thesaurus.com/browse/protest>

Link 5: <http://www.protest.net/>

3rd query – “Syria”.

Subject 1:

Link 1: <http://www.bbc.co.uk/news/world-middle-east-34784276>

Link 2: <http://www.theguardian.com/world/syria>

Link 3: <https://en.wikipedia.org/wiki/Syria>

Link 4: <http://www.bbc.co.uk/news/world-middle-east-34781225>

Link 5: <http://www.telegraph.co.uk/news/worldnews/middleeast/syria/>

Subject 2:

Link 1: <http://www.bbc.co.uk/news/world-middle-east-34784276>

Link 2: <http://www.theguardian.com/world/syria>

Link 3: <https://en.wikipedia.org/wiki/Syria>

Link 4: <http://www.bbc.co.uk/news/world-middle-east-34781225>

Link 5: <http://www.telegraph.co.uk/news/worldnews/middleeast/syria/>

Subject 3:

Link 1: <http://www.bbc.co.uk/news/world-middle-east-34784276>

Link 2: <http://www.theguardian.com/world/syria>

Link 3: <https://en.wikipedia.org/wiki/Syria>

Link 4: <http://www.bbc.co.uk/news/world-middle-east-34781225>

Link 5: <http://www.telegraph.co.uk/news/worldnews/middleeast/syria/>

References:

BBC News. 2015. GCHQ censured over sharing of Internet surveillance data with US. [online] Available from:

<http://www.bbc.co.uk/news/uk-31164451>

BBC News. 2015. TalkTalk cyber-attack: Website hit by 'significant' breach [online] Available from:

<http://www.bbc.co.uk/news/uk-34611857>

Beck U. 1992. Risk Society: Towards a New Modernity: Logic of wealth and risk distribution. Sage Publications LTD. P.1 & 21. Available from:

<https://books.google.co.uk/books?id=W2sDTHaSiiYC&printsec=frontcover&dq=risk+society+towards+a+new+modernity&hl=en&sa=X&ved=0CCIQ6wEwAWoVChMIjKLhPqGyQIVzLIUCh3vAQ8N#v=onepage&q=risk%20society%20towards%20a%20new%20modernity&f=false>

Graham D. 2014. The Atlantic. Rumsfeld's Knowns and Unknowns: The Intellectual History of a Quip [online]. Available from:

<http://www.theatlantic.com/politics/archive/2014/03/rumsfelds-knowns-and-unknowns-the-intellectual-history-of-a-quip/359719/>

Ha A. 2014. Tech Crunch. Edward Snowden's Privacy Tips: "Get Rid Of Dropbox," Avoid Facebook and Google. [online]. Available from:

<http://techcrunch.com/2014/10/11/edward-snowden-new-yorker-festival/>

Mirani L. 2013. Quartz: Between a quarter and a third of everything on the web is copied from somewhere else [online]. Available from:

<http://qz.com/159350/between-a-quarter-and-a-third-of-everything-on-the-web-is-copied-from-somewhere-else/>

Pariser E. 2011. The Filter Bubble: What the Internet Is Hiding From You. Introduction. Penguin. P.19

Pariser E. 2011. Ted: Beware online “filter bubbles” [online]. 03.21 mins, 04.05 mins, & 05.59 mins. Available from:

https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en

Rumsfeld D. 2007. Youtube: Donald Rumsfeld Unknown Unknowns! [online].

Available from:

<https://www.youtube.com/watch?v=GiPe1OiKQuk>

Seemann M. 2015. Digital Tail Spin: Ten Rules for the Internet After Snowden. Introduction. Institute of Network Cultures. P.9. P.10. P.26. P.53.

Smith C. 2015. BGR. Snowden discusses a scary way spies can hack your smartphone and gain ‘total control’ [online]. Available from:

<http://bgr.com/2015/10/12/iphone-android-smurf-spy-malware/>

Snowden E. 2015. Youtube: Live Q&A: Edward Snowden [online]. 10mins. Available from: <https://www.youtube.com/watch?v=IhKXTVc5h4A>

Taleb N. 2007. The Black Swan: The Impact of the Highly Improbable. Prologue: On the Plumage of Birds. Penguin. P. xvii, 30.

The Telegraph. 2015. Internet firms to be banned from offering unbreakable encryption under new laws. [online]. Available from:

<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11970391/Internet-firms-to-be-banned-from-offering-out-of-reach-communications-under-new-laws.html>

Timm T. 2014. The Guardian: First Snowden. Then tracking you on wheels. Now spies on a plane. Yes, surveillance is everywhere [online]. Available from:

<http://www.theguardian.com/commentisfree/2014/nov/15/spies-plane-surveillance-us-marshals>

Weaver M. 2015. The Guardian: UK public must wake up to risks of CCTV, says surveillance commissioner [online]. Available from:

<http://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent>

Wsystems. 2010. Surveillance. Types of surveillance: Cameras, Telephones, etc [online]. Available from:

<http://www.wsystems.com/news/surveillance-cameras-types.html>