WikiLeaks, Snowden and the fight to get the balance right: Information Asymmetry

2013 Whyte Memorial Lecture
Cassie Findlay

It is a tremendous honour for me to be delivering the Jean Whyte Memorial Lecture. I’d like to thank Professor Garcia de la Banda, Professor Sue McKemmish and the Committee for the invitation.

I’d also like to acknowledge Professor Jean Whyte and her sister Phyllis White, without whom I would not be here tonight. In finding out more about Professor Whyte, I was pleased to see that one of the projects funded by the Jean Whyte Fund for research into Librarianship, Archives and Records at Monash University is a PHD project on the role of records and information management as a support to corporate transparency. Amongst other goals, the work is designed to offer insight into better ways of keeping records which provide evidence of corporate activities that have an impact on the environment, human rights, and public health and safety. As someone who has a great interest in the co-dependency of justice and recordkeeping this seems to me a wonderful use of these funds.

This is a talk about information. Who has it, how they are getting it, and how they use it. It is about information and power, and it is about an emerging gap between what is made available to us and what we expect; between our expectations of privacy and the massive interception and collection of data on our every act online. It’s about surveillance and secrecy, and yes secrecy about surveillance. It’s about a gap, a ‘no mans land’ where a war has been quietly raging for years, with many of us only waking up to it now.

We are in the midst of a form of information asymmetry at a scale that we have simply not seen before. In contract theory and economics, information asymmetry deals with the study of decisions in transactions where one party has more or better information than the other. This creates an imbalance of power in transactions, which can sometimes cause the transactions to go awry, a kind of market failure in the worst case. If we consider transactions that occur in other aspects of society, the same rule holds. Where better, more accurate or more information is held by one group, they wield power over the other. Of course through history there has always been secret dealings of the powerful and carefully controlled ignorance of those under their control. This is not new. What is new, I would argue is the scale of the one way flow of information from us to ‘them’-, to the behemoths of industry of the internet age, and to our governments.

A few observations illustrate this:

- Right now, Google knows more about you than probably your mother does.
- The Obama administration has now charged more whistleblowers under the 1917 Espionage Act than all previous administrations combined. Including Bradley Manning and most recently Edward Snowden. This was the Act under which the Pentagon Papers’ Daniel Ellsberg was charged in 1971.
- Secret courts in the United States are compelling Google (and Yahoo) to hand over data on what you do online right now. They (Google etc) are not allowed to talk about this beyond a few basic facts.
- By last year Britain’s spy agency GCHQ tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time. Each of the cables carries data at a rate of 10 gigabits per second, so the tapped cables had the capacity, in theory, to deliver
more than 21 petabytes a day – equivalent to sending all the information in all the books in the British Library 192 times every 24 hours.¹

- Free press organisation, WikiLeaks who publish leaks from whistleblowers is blockaded financially, with all major credit card companies bowing to political pressure and refusing to process payments to them since December 2010.
- The vast majority of the records of acts and deliberations of Australian government, Local, State and Federal are still kept hidden from public view for a default 20 or 30 years, despite attempts to make more available under reformed FOI laws. Further discussions of reform to FOI in many western democracies indicate an appetite for winding back

Information asymmetry indeed.

It was the arrival of WikiLeaks on the world stage which really caused me to start thinking more deeply about this stuff. There I was in 2010, a mild mannered archivist, working with organisations to make, keep and share digital records more effectively and planning to implement a digital archive for the NSW Government when WikiLeaks changed the game. During interviews about the massive releases of that year, Julian Assange spoke of the availability of ‘the historical record’- even if it relates to events of yesterday. The Manning leaks were entire archives - for me, while the secrets they revealed were stunning (sometimes in their triviality - why on earth were they classified?), I found examination of them from a recordkeeping perspective just as fascinating.

My interest in the goals of WikiLeaks for the availability of information to achieve justice chimed with my interest in the use of archives in addressing past human rights abuses as we have seen in places like South Africa with the Truth and Reconciliation Commission and the Secret Police Archive in Guatemala. And in the need for our profession to embrace and exploit the digital age, stepping away from methods built for the paper world. Thinking and writing about WikiLeaks and archives eventually resulted in a few meetings over the last couple of years with Julian Assange and the opportunity to discuss some of these questions with him. It also lead to my involvement in the establishment of the WikiLeaks Party in Australia. A party not without its challenges in its formative stages, but something that I am very proud of having helped to set up. The vision is for a political manifestation of what WikiLeaks has done in journalism and publishing. The WikiLeaks organisation was pioneering in its use of ‘scientific journalism’, reporting information with reference to publicly available primary sources. The WikiLeaks Party promotes ‘scientific policy’; decision-making based on research, evidence and clear, transparent principles. A step away political party oligarchy, in which dissent is stifled and the public bureaucracy is contained and docile.

Of course as lead candidate in Victoria, Julian worked very hard on presenting the ideas of the party through the campaign period, but others from WikiLeaks were involved too. In the middle of the year, WikiLeaks journalist Sarah Harrison assisted us with various infrastructure matters. One day, and very apologetically, she explained that she had turn her attention elsewhere. The next time I spoke with her directly was after she had been allowed to leave Sheremetyevo Airport with Edward Snowden after being trapped there for 39 days after the US cancelled Snowden’s passport preventing him from travelling to Latin America as planned.

---

¹ Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball ‘GCHQ taps fibre-optic cables for secret access to world’s communications’ The Guardian, Saturday 22 June 2013 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

This is a picture from an event in Moscow where Edward Snowden received the Integrity Award from the Sam Adams Associates for Integrity in Intelligence. Sarah is second from the left. Sarah recently issued a statement on arriving in Berlin, where she has gone after her lawyers advised her that her work to support Snowden could result in her being charged under the UK Terrorism Act and that it is not safe for her to return home.

“In these times of secrecy and abuse of power there is only one solution – transparency. If our governments are so compromised that they will not tell us the truth, then we must step forward to grasp it. Provided with the unequivocal proof of primary source documents people can fight back. If our governments will not give this information to us, then we must take it for ourselves.

When whistleblowers come forward we need to fight for them, so others will be encouraged. When they are gagged, we must be their voice. When they are hunted, we must be their shield. When they are locked away, we must free them. Giving us the truth is not a crime. This is our data, our information, our history. We must fight to own it.”

I would encourage you all to read her inspiring statement, available on WikiLeaks’ website

Of course Snowden and the NSA files are amongst the biggest news stories worldwide this year. Thanks to the courage of Edward Snowden and the work of journalist Glenn Greenwald and others we have learned (and continue to learn) of the stunning overreach of the United States’ National Security Agency - secret and warrantless surveillance in concert with internet giants and in partnership with foreign security agencies eg GCHQ, ASIO have demonstrated US and other Western governments’ determination to know what we are doing online, all the time.

Under PRISM, the NSA gathers huge volumes of online communications records by legally compelling US technology companies, including Yahoo! and Google, to turn over any data matching court-approved search terms. That program is authorised under Section 702 of the Foreign Intelligence Surveillance Act and overseen by the Foreign Intelligence Surveillance Court - a court which can carry out such authorisations out of the gaze of the public eye.

More recently leaks revealed that the NSA also intercepts traffic apparently without any knowledge of these internet giants by secretly breaking into the main communications links that connect Yahoo! and Google data centres around the world. We know from documents leaked by Snowden that Britain’s spy agency GCHQ has secretly gained access to the network of cables which carry the world’s phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner, the National Security Agency (NSA).

The sheer scale of the agency’s ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. One key innovation has been GCHQ’s ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months. GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely innocent people, as well as targeted suspects. This includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user’s access to websites – all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets.

---

There is every reason to suspect that all the countries of the 5 eyes alliance are similarly tooled up for this level of surveillance and data retention, including Australia. And indeed we also now know that the NSA has gathered the calls of millions of French, German, Brazilian and other global citizens.

Edward Snowden has called this "the largest programme of suspicionless surveillance in human history". This is his key point. Not that it is happening, but all being carried out without any form of public acknowledgement or debate.

And while in more recent weeks our news has been dominated by new revelations from the Snowden leaks about the United States’ spying on world leaders, both friend and foe, and of Australia’s role as effectively a subcontractor for this dirty work in Asia (I enjoyed the Indonesian foreign minister’s recent protestation that it just wasn’t cricket), surely we are not surprised? World leaders have spied on one another since earliest civilisation. So while I do think it says something about American exceptionalism and makes for some fun (and mostly overblown) expressions of outrage from diplomats, it is not new. What is new is the scale and breadth of universal spying on all of us - made possible by the ubiquity of the internet and US owned internet giants, operating at the behest of an unaccountable and out of control security state.

The ripples around the globe from the Snowden material seem to be turning into waves day by day. Nation states are reacting with shock and anger to the revelations of just how much information gathering and privacy intrusion has been going on. Relations between many countries and the united states are now more strained than for a generation. Early on we saw a diplomatic crisis threaten when on July 2, the United States put pressure on several European countries to prevent a plane carrying Bolivian President Evo Morales from landing to refuel at any of their airports. The excuse for this unprecedented denial of landing rights was the unfounded claim that Morales was hiding American whistleblower Edward Snowden on board his presidential jet.

In Latin America this was just the start of diplomatic disquiet with the United States. Much of the discussion in these nations has concerned the very building blocks of the internet. Thirty five years ago, different countries had their own telecommunications infrastructure, so the division between foreign and domestic collection was clear. Today there's a global communications infrastructure, mostly centred around United States territory. 98% of Latin American telecommunications to the rest of the world - SMS, phone, email etc - passes through the US. IN a recent speech, the President of Brazil Dilma Rousseff called for the creation of an independent internet and communications platform within Latin American nations, not subject to US control.

Potential for the Balkanisation of the internet as a push back against US control and interception is also seen in the cloud computing market. A European Commission memo issued this year pointed to ‘recent revelations about PRISM and other surveillance programmes’ as impeding the take up of cloud services, and encouraging a growth in national or regional cloud computing initiatives. The EU wants Europe to embrace cloud computing - using a European based ‘secure’ cloud, replete with European data protection laws and out of the grasp of the NSA or the Patriot Act.

Brazil is also, with Germany working on a UN General Assembly resolution to highlight international anger at US data spying in other countries. The draft calls for an end to excessive electronic surveillance, data collection and other gross invasions of privacy. It does not name any specific countries, although U.N. diplomats have said it was clearly aimed at the United States. The German-

---

Brazilian draft would have the 193-nation assembly declare that it is "deeply concerned at human rights violations and abuses that may result from the conduct of any surveillance of communications". There is likely to be widespread support for adopting the resolution.

Brazil has also put their ‘Marco Civil’ internet freedom legislation back on the agenda – this is a remarkably progressive bill to protect online freedoms which for the past 3 years has remained stuck in Parliament, under heavy pressure by industry – mostly telecom – lobbies.

Germany, Brazil’s partner in the UN resolution, has become a safe haven for several key players in the Snowden case including filmmaker Laura Poitras and Sarah Harrison. Just last week Der Spiegel urged asylum for Snowden in its cover story. In the UK however: Prime Minister David Cameron has called on the Guardian and other newspapers to show "social responsibility" in the reporting of the leaked NSA files to avoid high court injunctions or the use of D notices to prevent publication in a statement to MPs on he warned of the dangers of a "lah-di-dah, airy-fairy view" about the dangers of leaks.

And in Australia? Reactions here have been I would suggest, muted. Perhaps in the age of an Abbott Government and with our Murdoch saturated press this is not surprising. When challenged by the media and in Parliament on the question of whether Australian intelligence agencies were receiving information from the PRISM program, successive Attorneys General have refused to confirm or deny. Greens Senator Scott Ludlam has called for a parliamentary inquiry into Australia’s participation in spying with the National Security Agency (NSA), similar to investigations being held in the UK, Spain, Germany and the US. Such an inquiry seems unlikely to proceed.

What the NSA leaks have demonstrated with clarity I think is that we are the prisoners in a global internet panopticon. As expressed by Foucault, the Panopticon creates “a consciousness of permanent visibility as a form of power, where no bars, chains, and heavy locks are necessary for domination any more.” Security agencies say the data they collect is retained so they can investigate criminal matters - including crimes not yet suspected. Retention periods they get vary, for the Tempora program it’s just 30 days, Nicola Roxon wanted two years for communications and ISP metadata - in fact the head of the AFP wanted it all to be kept indefinitely.

Of course, this kind of bulk information gathering and retention is not a new concept. “Mosaic theory” describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Mosaic theory was what caused intelligence organisations like Australia’s ASIO (Australian Security and Intelligence Organisation) in the mid 20th century to record what seemed like incredibly mundane activities and communications of what were then called ‘persons of interest’. For example, continuous surveillance of the doorway to Sydney’s Communist party headquarters – for decades. Or activists like Gary Foley were tailed and photographed as they went about their daily lives.

What was recorded now tells us more about the changing state of fashion than it ever told us about the (hardly dangerous) activities of those who came and went. But for ASIO, the game was to gather

---

5 EFF ‘Brazil and Germany Proposed UN Resolution Against Mass Surveillance’, November 12, 2013

as much as they possibly could. Not only to attempt to build a bigger picture in line with mosaic
theory, but more prosaically, to keep themselves in work in the relatively unexciting backwater – in
espionage terms – that Australia was in the 1950s, 60s and 70s.

As we can see now from the ASIO archives, these surveillance activities produced mammoth
quantities of records – in the form of telephone conversation recordings and transcripts,
photographs, film and copies of press clippings. These were carefully gathered, collated and filed.
And then, for the most part, the information sat unloved in the files unless some alert intelligence
officer happened to think of some way to link a new discovery to something previously recorded.
They simply did not have the tools to analyse the information they had.

With Snowden leaks we have seen the universal surveillance state that we now live in. No longer are
spying activities limited to ‘persons of interest’; we are all persons of interest. Technology has
allowed State and corporate actors to implement mosaic theory on a scale never dreamt of by the
spies of the Cold War. Whole countries’ communications are tracked and recorded, and the data is
stored so that it can be mined for random mentions of key words which, when matched with
perhaps an email, a tweet or a mobile phone call, will set off an alarm bell.

Some people will say this is a sacrifice to our civil liberties that we must accept if we are to be safe.
Indeed, when promoting the data retention aspects of the national security legislation reforms her
government proposed, former Attorney General Nicola Roxon’s consistent message to sell her
proposed reforms to national security legislation7 was that we must be prepared to accept some loss
of civil liberties if we are to feel safe in the modern world of cyber terrorism. However the kinds of
reforms being proposed and the actions we have seen revealed by Snowden are about more than
modernising existing surveillance powers. They are about enabling secret, warrantless mass
surveillance and data retention. What David E Pozen termed ‘adversarial mosaic-making and
informational paranoia’ in a 2005 article in the Yale Law Journal8 is just one of the many aspects of
the state of universal surveillance we live in that has been brought to light by Edward Snowden. It is
easier than ever before for repressive regimes, companies and our government here in Australia to
establish the mechanisms necessary to create a digital archive on any of us to be used for unknown
purposes in the future. Information paranoia indeed.

Free software pioneer Richard Stallman recently neatly summed up the link between surveillance
and the fight for transparency of powerful institutions:

“...If whistleblowers don’t dare reveal crimes and lies, we lose the last shred of effective
control over our government and institutions. That’s why surveillance that enables the state
to find out who has talked with a reporter is too much surveillance — too much for
democracy to endure.”9

---

7 Joint Parliamentary Committee on Intelligence and Security, Inquiry into potential reforms of National
Security Legislation
s/nsl2012/index.htm

115:628, 2005

http://www.wired.com/opinion/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-
surveillance/
You might say well, our government is democratically elected, we have checks and balance in place, I am happy to trust that their motives and acts are for my good. But I suppose what I would argue is that the shifting in the balance of information and therefore power that has been occurring, hardly perceptible before, much more dramatically observed now, is part of a move in the wrong direction for us as a society.

There are two sides to this: First, the degradation of our human right to privacy, so eloquently presented by Louis Brandeis, who, in his 1890 treatise with Samuel Warren write these words:

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual ... the right ‘to be let alone’ ... Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”¹⁰ (He was speaking of the invention of the portable camera and celebrity journalism of the day!)

The other side is the information blockages which offer the opportunity for states to engage in more conspiratorial behaviours, inherently at odds with the will of the people.

This was an idea put forward by Julian Assange in his 2006 essay ‘Conspiracy as Governance’:

“Plans which assist authoritarian rule, once discovered, induce further resistance. Hence such schemes are concealed by successful authoritarian powers until resistance is futile or outweighed by the efficiencies of naked power.”¹¹

He goes on to quote Machiavelli:

“Thus it happens in matters of state; for knowing afar off (which it is only given a prudent man to do) the evils that are brewing, they are easily cured. But when, for want of such knowledge, they are allowed to grow until everyone can recognise them, there is no longer any remedy to be found.” *(The Prince, Niccolo Machiavelli [1469-1527])*

So we understand much more now about how much information about us and from us is available to tens of thousands of security agency staff, tech companies, contractors and ISPs. Conversely, how much do we know about them? About Machiavelli’s ‘evils that may be brewing’? What do we know of the guards of our panopticon? How are we able to learn about them?

Well, we have Freedom of Information (FOI). FOI is predicated on the assumption that a community that is better informed can participate more effectively in the nation’s democratic processes, and that information gathered by government at public expense is a national resource and should be available more widely to the public

FOI and privacy laws provides a mechanism for individuals to see what information is held about them on government files, and to seek to correct that information if they consider it wrong or misleading.

---


¹¹ Julian Assange ‘Conspiracy as Governance’ December 3, 2006

However as someone who closely follows FOI implementation and proposals for its reform, I have seen not only a lack of political will to reveal seriously damaging information but many practical barriers that there is no appetite to remove.

Just last week a journalist I know reported that in researching a story on children in detention centres, DFAT rejected a request for certain data on children in detention on the basis that the records did not permit it to be efficiently extracted – it would be too great a burden on the agency. In my experience, this can be the result of lack of will to disclose, either the narrow definition of FOI as pertaining to documents or poorly designed digital recordkeeping systems. Whatever the reason, these are the sorts of barriers which many of us made submissions on in the Hawke review of Commonwealth FOI legislation. It would seem unlikely that the current government will take them up. Indeed, even in governments who were actively arguing for better FOI we see a retreat from it once in power – Tony Blair, the architect of FOI in the UK recalled in his memoir that he called himself “an idiot; a naive, foolish, irresponsible nincompoop”\(^\text{12}\) for having brought it in in the first place.

Australia has failed to join the Open Government Partnership and seems unlikely to do so now. However how much of this is real change and how much is spin? The Open Government Partnership Summit was held in London two weeks ago. Reflecting on it, Alex Howard of Columbia University queried whether we are experiencing ‘peak open’:

> “Scrolling back through thousands of #OGP13 tweets, watching conference pictures, or reading the summit agenda or fact sheets doesn’t capture the mix of excitement, optimism, skepticism and anger that attendees could feel on every floor of the conference. Swirling underneath the professional glitz of an international summit were strong undercurrents of concern about its impact upon governments reluctant to cede power, reveal corruption or risk embarrassment upon disclosure of simple incompetence. The OGP summit took place at a moment where 21st century technology-fuelled optimism has splashed up against the foundations of institutions created in the previous century.”\(^\text{13}\)

I would argue that governments here, in the UK, the US and elsewhere are making grand pledges of greater openness which many see as not backed up by serious commitment to the principles of openness, particularly in relation to policy and law that is pushing at or breaking the boundaries of public expectations.

Tim Berners Lee, the inventor of the world wide web, made this observation recently: comments re whistleblowers and inadequate accountability, shown in what Snowden revealed of security agencies’ overreach:

\(^{12}\) Martin Rosenbaum, ‘Why Tony Blair thinks he was an idiot’, BBC News Open Secrets 1 September 2010 [http://www.bbc.co.uk/blogs/opensecrets/2010/09/why_tony_blair_thinks_he_was_a.html](http://www.bbc.co.uk/blogs/opensecrets/2010/09/why_tony_blair_thinks_he_was_a.html)

“It’s clear that the systems in the U.S. and UK have not been good enough. The systems of accountability have failed,” he said. “In the future, what we have to do is set that system up.”

We are seeing more aggressive moves to silence whistleblowers, attacks on free press and over the top punishments for information activists.

This is Thomas Drake, a former senior executive of the U.S. National Security Agency (NSA), a decorated United States Air Force and United States Navy veteran, and a whistleblower. In 2010 he was indicted with charges relating to retaining national security information. He has said he was persecuted for challenging the NSA’s Trailblazer data collection program, and in speeches has said to his audience: "Put your entire life in a box, your documents, bank accounts, your passwords, everything -- and give it to a complete stranger -- a fellow American for safekeeping. Would you do it?” he states that he has yet to encounter a “yes”.

This is Jeremy Hammond. Due to be sentenced this week, he is currently facing federal criminal charges for allegedly leaking documents of the private spying agency Stratfor through Wikileaks. Charged under the US Computer Fraud and Abuse Act, Jeremy has, since March 2012, been denied bail, cut off from his family, and held in solitary confinement. He is facing a maximum sentence of ten years.

This is Chelsea (formerly Bradley) Manning, who leaked the collateral murder video, military records from the Iraq and Afghan wars and state dept cables to Wikileaks. He was recently sentenced to 35 years in military prison. In a statement read at his sentencing, Manning said:

“Whenever we killed innocent civilians, instead of accepting responsibility for our conduct, we elected to hide behind the veil of national security and classified information in order to avoid any public accountability.

When I chose to disclose classified information, I did so out of a love for my country and a sense of duty to others.

If you deny my request for a pardon, I will serve my time knowing that sometimes you have to pay a heavy price to live in a free society.”

There are those who would argue that we must fight for better FOI laws, whistleblower protections – including for the military and security agencies - stronger shield laws for journalists, and a rebalancing of the weighting given to computer crime which often results in disproportionately high sentences for internet activists. Yes, these are good things to fight for, especially to aim for uniformity here in Australia rather than the patchwork of laws we have at present, but there are others who do not believe our current political systems will enable true reform and that we must seek alternative means to claim our rights to information.

This is a tweet by activist, Grateful Dead lyricist John Perry Barlow which for me at the time (Dec 2010) summed up the situation: It is a war. The combatants are activists, journalists, hackers and publishers. They are Anonymous, they are cryptographers. They are lawyers and they are politicians. The battlefield is the courts, the board room, the parliament, the newsroom and the street. But most of all it is the internet. The gap - between what we know and what is known of us, between openness and secrecy, between a society in which whistleblowers and publishers may speak truth to

---

14 ‘We need whistleblowers’ says Web inventor Tim Berners-Lee’, Al Arabiya News, 23 October 2013
power and one in which they are persecuted creates a vacuum, or void. Internet activist Gregg Housh blogged about this recently, saying

“That void grew for years, and finally when we could stand it no more it got filled. The void was filled by Anonymous, Wikileaks, new Whistle-blowers, and a new prevalent culture of transparency.”

Many others have been inspired by WikiLeaks and are looking for new ways to share information that can ‘move the world’. Alexa O’Brien’s work recording every day of Chelsea Manning’s pre-trial hearings and trial, given that the military courts do not publish reports on these sessions. Alexa’s site has become the authoritative archive of this historic case. A journalism co-op starting up in Ecuador under the guidance of Australian journalist Austin Mackell that I am involved in – bringing primary sources to every story, my role that of manager of the ‘artefact cave’ where people can see for themselves the basis of the reporting. Projects like Detention Logs: a new project supporting deeper community knowledge of and accountability for conditions in Australia’s immigration detention network. The project embraces WikiLeaks’ philosophy of scientific journalism by using primary materials, largely the results of FOI requests, gathered and formatted at scale, to show the inside view as opposed to the spin. Activist and lobbying groups like the EFF, the Freedom not fear day of action, campaigns against internet filtering, surveillance and data retention. Whistleblower projects like GlobalLeaks, BalkanLeaks, Tahrir Square’s 25Leaks. I note just in the last week the appearance of ‘MafiaLeaks’.

At the same time, activists are building and sharing the tools needed to grasp Brandeis’s ‘right to be let alone’ in the online world. These are activists concerned with the use of encryption for communicating, sharing information and organising. Emerging out of the ‘cypherpunks’ movement, they understand that the internet, once so full of promise, has become a trap for dissenters and resisters. Secure email and browsing capabilities become crucial in countries with oppressive regimes, but increasingly activists in all settings use them as a matter of course. This includes tools like Tor, OTR, silent circle and others. The ‘cytoparty’ project, started here in Australia spread quickly worldwide as a way to share knowledge about how to use tools like these (and drink beer). Another of the motives for the current level of surveillance of the internet is that sites are financed through advertising based on tracking users’ activities and propensities. Privacy of internet commerce has had its roots in sites like Silk Road, and the internet currency Bitcoin.

There are so many other ways that our identities and lives are tracked, recorded, stored its mind boggling – from smartphones to electronic transport cards. It is almost impossible to imagine living unrecorded. But these and other projects uphold that it is our right and will keep working to try to achieve it.

Where will this go? Are the mega internet companies’ grips on our data, the economic drivers at play and the fundamental nature of the infrastructure of the internet so established that we are inevitably destined for a global surveillance dystopia?

Taking part in the fight for internet freedom, free speech and the right to know can seem like the proverbial finger in the dyke at times. And the plight of people like Chelsea Manning, Jeremy Hammond, Edward Snowden and Julian Assange can be sobering for even the hardiest of souls.

15 Gregg Housh ‘The Vacuum That Created Anonymous, Wikileaks, and the Whistleblower Explosion’ October 27, 2013 http://0v.org/
But, to return to the Panopticon, courageous publishers like WikiLeaks whistleblowers like Edward Snowden and information activists are turning the lights on in the guard tower. What we, the watched prisoners, choose to do about what we see there, will shape all of our futures.