Surveillance & Society

Editorial | Before and After Snowden

David Murakami Wood

Surveillance Studies Centre, Queen's University, Canada.
dmw@queensu.ca

Steve Wright

Leeds Beckett University, UK.
s.t.wright@leedsbeckett.ac.uk

In retrospect, it seems somewhat premature to have issued a call on Surveillance and Security Intelligence *after* Snowden. At the time of writing, despite his enforced exile in Russia, former National Security Agency (NSA) contractor and whistleblower, Edward Snowden, seems almost ubiquitous as a participant in debates on transnational surveillance, even appearing virtually on one occasion in a Canadian High School (Bradshaw 2015). And, as with all such impromptu historical periodizations, there is always also a case to be made to say that Snowden's revelations didn't change as much as we thought it might, or at least, rested on a legacy of former events or long-standing processes. In the case of surveillance and security intelligence, the latter is certainly true. The former remains open as revelations and discussion resulting from both the documents taken by Snowden continue in the broader context of the changed climate of transparency resulting from his revelations and other major initiatives like *Wikileaks*. In particular, new documents and ongoing analysis can be found in Glenn Greenwald's online intelligence news source, *The Intercept*, and in newspapers like *The Guardian* in the UK, *Der Spiegel* in Germany, and the *Washington Post* in the USA.

There is a history of revelation and whistleblowing about the NSA as long as the history of the agency itself[1]. Founded in 1952, information about the NSA began to emerge almost immediately afterwards. Particularly embarrassing was a spy scandal in 1960, when two employees, William Martin and Bernon Mitchell, defected to the Soviet Union. However it was not until the 1970's that the agency became more widely known among researchers, journalists and activists. A series of articles in the *New York Times* in 1971 threatened to reveal, amongst other revelations in 'The Washington Papers about the Vietnam conflict, the ability of the NSA to listen in on the scrambled telephone conversations of Soviet officials. The NSA took various forms of legal and intimidatory action and managed to prevent publication of the offending aspects (Bamford 1982).

This stillborn mainstream American reportage was followed by an article in the radical magazine, *Ramparts*, in August 1972, purporting to be the revelations of one 'Winslow Peck' (later identified as a Washington lobbyist with the equally colourful real name of Perry Fellwock). Much was confirmed by another anonymous ex-NSA whistle-blower in an interview with Australian magazine, the *Nation Review*, which revealed far more of the international networks of intelligence gathering presided over by the NSA, indicating the extent to which other domestic intelligence services were subject to the policy and operational direction of the NSA, and hinting at the large number of bases throughout the world at which the NSA operated.

[1] The pre-2000 history here is largely based on Wood (2001) and Wright (2005).

Murakami Wood, D. and S. Wright. 2015. Editorial: Before and After Snowden. *Surveillance & Society* 13(2): 132-138. http://www.surveillance-and-society.org | ISSN: 1477-7487

By 1975 the concern caused by the various reports, of which those about the NSA were only small part, was such that it led to a slew of official investigations, a period termed the 'Season of Inquiry' by American intelligence researcher, Loch Johnson (1988). The most important were The Pike Committee in the House of Representatives, in which the first official reference was made to the NSA's international telephone tapping operations; the Church Committee in the Senate, which revealed joint NSA-FBI operations against US citizens – mainly activists from the student, civil rights, and the black and red power movement; the Abzug Committee in the House of Representatives, which focused on the NSA's International Licensed Cable (ILC) tapping of undersea cables, which is still the basis for much of the NSA's Internet tapping; and finally, an Inquiry by the Attorney General.

The mass of evidence uncovered by these Inquiries meant that by the late Seventies some regulation of the NSA was inevitable. The eventual result was the Foreign Intelligence Surveillance Act (FISA) of 1978 under the liberal Democratic administration of Jimmy Carter, which provided some very limited controls that were easily bypassed by the NSA. The FISA also established the Federal Intelligence Surveillance Court (FISC), whose handpicked judges met in secret in the Justice Department to decide on applications for surveillance involving American citizens. According to all reliable commentators, no application has ever been refused by the FISC.

However, the Season of Inquiry inspired further investigation of security intelligence. Several were crucial. The first was the work of New York lawyer and ex-intelligence services employee, James Bamford, who in 1982 published what was for years the only serious book-length exploration of the NSA, *The Puzzle Palace*. This was finally followed up with *Body of Secrets* in 2002 and then *The Shadow Factory* in 2008. The 1980s also saw the crucial investigative work of Jeffrey Richelson and Desmond Ball (1985), which detailed the locations and functions of major NSA bases around the world, and most importantly outlined the existence and functions of the until then entirely secret 1946 UKUSA agreement on Signals Intelligence sharing, with its first and second parties, now more often referred to as the 'Five Eyes': the USA, UK, Canada, Australia and New Zealand.

Some investigative journalists and campaigners went further, in particular, Scottish investigative journalist, Duncan Campbell. Campbell's first major involvement in this area was in the research for an account of GCHQ's role and functions, which led writing an article about GCHQ, *The Eavesdroppers*, with the American journalist, Mark Hosenball, for London's Time Out magazine in 1976. This was the first comprehensive account of what GCHQ was, and what it did, and some information about links to the NSA, and included material from an interview with 'Winslow Peck'. This was the beginning of a process which lead to the infamous ABC trial, which saw Campbell prosecuted by the British State in 1977, along with fellow journalist Crispin Aubrey and former British army intelligence operative, John Berry. Hosenball was deported.

Campbell was not put off by his prosecution. In 1980, with Linda Melvern, Campbell wrote the first public account of the NSA's major European base, Menwith Hill in North Yorkshire, UK, 'America's Big Ear on Europe' for *New Statesman* magazine, upon which he expanded in *The Unsinkable Aircraft Carrier* (1984). This work was partly based fieldwork on secret UK telecommunications systems that had been conducted by Steve Wright in the 1970s for his doctorate (Wright 2005). Later in the 80s, Campbell produced another article for *New Statesman*, 'They've Got it Taped', revealing a system of computer-aided traffic analysis called P415 by NSA contractor, Lockheed. This later became known to the public as ECHELON, as a result of work done in collaboration between Campbell and peace activists at Menwith Hill, who reconstructed shredded documents discovered in the waste bins of the base with forensic accuracy. The immediate result of this research was *The Hill*, a documentary for the UK's Channel Four. The film featured the first really systematic picture of what happened inside the NSA, and named ECHELON and the systems of which it was part worldwide.

Campbell's informant on P415, was later revealed to be Margaret Newsham, who was perhaps the most celebrated NSA whistle-blower before the 2000s. Newsham was a computer software systems co-ordinator for Lockheed and a several other companies contracted to provide services to the NSA from 1974, and was responsible for the VAX computers on which ECHELON was developed (Elkjaer and Seeberg 1999) She came to prominence by giving evidence on the abuses she claims to have witnessed to an in-camera House Permanent Select Committee on Intelligence session in 1988. What she said is still secret but caused utter shock in the committee, according to her first major television interview, in an episode of American television network CBS's *Sixty Minutes* (CBS 2000), which also contained further confirmation of her story from another whistleblower, the former Communications Security Establishment Canada (CSEC) employee, Mike Frost.

Other important investigators include the New Zealand peace activist and investigative journalist Nicky Hagar. In 1996 Hagar published *Secret Power*, which was the first account of the real nature of relationships between the Five Eyes. Hagar showed how intelligence priorities that were actually relevant to New Zealand and to the Pacific nations more generally were systematically excluded in favour of American priorities. The book also revealed the nature and extent of ECHELON, and how it operated through 'Dictionaries' specific to each UKUSA party. The book was published by a very small press, and it was not until Steve Wright picked up on Hagar's article for the first official European Parliament (EP) report on ECHELON*, An Appraisal of the Technologies of Political Control* (Wright 1998), that his work became truly appreciated. The EP also published the summation of Campbell's work, *Interception Capabilities 2000* (Campbell 1999), and embarked on a series of inquiries into ECHELON, a history of which has just been produced by the European Union's archives services (Piodi and Mombelli 2014).

While these and other national parliamentary inquires put knowledge about the NSA in the public domain, most of the primary research on the NSA and its networks before Snowden came from parapolitical organisations: investigative journalists, activists and whistle-blowers have increasingly created structures through which they could find support, continue their work, and more effectively challenge and influence official discourse. These include, in the UK, Tony Bunyan's Statewatch, which was founded as a direct result on the ABC Trial, and which continues to concentrate on European security, surveillance and political policing, and has uncovered a great deal about secret EU-FBI policing cooperation in particular and produced excellent work on the 'security-industrial complex' (Hayes 2009), mapping links between state and private security and surveillance organisations. Privacy International (PI), formed by Simon Davies in 1990, which campaigns against monitoring and surveillance of individuals by the state, and by private corporations, has also been particularly important in bringing the Five Eyes network to the attention of legislatures on both sides of the Atlantic. And there are less public organisations, for example the Omega Research Foundation, which has worked quietly away for many years, often undercover, on a range of security and surveillance topics.

In the USA, there is the Electronic Privacy Information Centre (EPIC), founded in 1994, and which has employed many of the most important researchers and whistleblowers in this field including Duncan Campbell and Wayne Madsen (see below) and the American Civil Liberties Union (ACLU), which is a much older civil rights organisation that has been crucial in getting attention to surveillance concerns in the US Congress. Increasingly important in recent years has been the Electronic Frontier Foundation (EFF). A key organisation from the anti-militarism rather than a pro-privacy tradition was the Federation of American Scientists (FAS), which began life as the Federation of Atomic Scientists. FAS used to employ John Pike as an intelligence researcher, but he has since formed his own research consultancy, Global Security. Also vital here is Cryptome, John Young's New York-based on-line cryptology information server, which deserves more credit for doing what Wikileaks is doing before Wikileaks.

Prior to 9/11, perhaps the single most in-depth account was a series of articles called 'No Such Agency' (Shane and Bowman, 1995) published by the *Baltimore Sun*, the 'local paper' of the NSA. Over a decade

after *The Puzzle Palace*, the pieces summarised most of the Bamford and Campbell material and provided histories of the NSA, including some newer allegations particularly over the NSA's subversion of the leading international cryptographic equipment supplier Crypto AG and world-leading software provider, Microsoft. These allegations were expanded upon by the whistle-blower who, prior to the 2000s, was the most vociferous critic of the NSA, Wayne Madsen. Having joined the NSA in 1975 via the US Marine Corps and later like Margaret Newsham, working for contractors, Madsen was responsible for much of the inside information in an article in the *Village Voice* (Vest and Madsen 1999), which detailed the role of the NSA in subverting UNSCOM, the United Nations chemical weapons inspection organisation in Iraq through its Special Collections Service. However Madsen and Newsham's stories were publicized more fully in Denmark than anywhere else: Bo Elkjaer and Kenan Seeberg for *Ekstra Bladet* in Denmark wrote hundreds of articles on the NSA, ECHELON and the place of Denmark as a typical 'third party' to the UKUSA agreement. Other 'third parties' include major industrial powers like Japan and Germany, but not France, which has resisted being drawn into what it sees as an 'Anglo-Saxon' system.

It is clear that public knowledge of transnational intelligence services surveillance systems had already changed before 9/11. Newspapers were printing stories about the NSA more regularly; activists and whistleblowers were getting a hearing. 9/11 saw a retrenchment and a fight-back by the USA and its Five Eyes allies, with new secret authorisations and programs, and a renewed commitment to funding and defending not just existing security intelligence bodies like the NSA and the CIA but an entirely new set of organisations around Homeland Security.

However, with hindsight, 9/11 seems less like a transformative trigger event for surveillance, an axis around which 'everything changed', and more like an opportunity for the confirmation and strengthening of existing trends, particularly a growing anxiety amongst intelligence agencies that the Internet both supplied them with an amazing new source of data, much of it 'freely given' by participants on social media, but also presented massive new problems in terms of being a space that was potentially unlimited and out of control. This was equivalent to the ambivalence about the so-called 'Revolution in Military Affairs' (RMA) that had been going on since the end of the Cold War. In an essay in the New York Times in October 2005, US military strategist, John Robb, argued that the Iraq war had turned into what he termed an 'open source insurgency': "a resilient network made up of small, autonomous groups" (Robb 2005). He argued that those resisting the US occupation and other armed groups were like open source software developers in that "the insurgents have subordinated their individual goals to the common goal of the movement."

For the Internet we have seen, and continue to see, attempts in multiple countries to attack the basis of what makes the Internet creative and free, in the name of all kinds of 'risks' (mainly terrorism, identity crime, intellectual property crime and paedophilia). Of course these risks are no greater on the Internet than in the material world, but the Internet is still for many people, and many politicians in particular, a vast 'terra incognita' that they do not understand. Here western governments are no different in their response to the government of China, if at least paying lip service to democracy and accountability. As an example, ex-NSA supremo and Vice-Chair of Booz Allen Hamilton, Mike McConnell, has been promoting the 're-engineering' of the Internet (Singel 2010) because the current openness of the Internet means that terrorists and criminals can flourish. This would "make attribution, geo-location, intelligence analysis and impact assessment – who did it, from where, why and what was the result – more manageable". In other words to close the Internet, remove everything that is innovative and democratic about it, and make it easier for agencies such as the NSA to monitor it. Along with a whole raft of measures like extending 'lawful access' regimes, introducing corporate-biased copyright and anti-peer-to-peer file-sharing legislation, censorship and Internet filtering, this is an attack on what the Internet has become and to turn it into something simply for consumption – something, in other words, more like a broadcast medium.

But at the same time, intelligence agencies had already worked out the advantages to be found in the massively increased availability of data from 'open source intelligence' (OSINT). Such actors also seem determined to store and fix ever-larger amounts of data in new repositories, for example the US National Security Agency's massive Utah data repository. This is all about leveraging the openness of the new networks, and using them to leverage 'big data', to connect and bring together otherwise unconnectable and widely distributed information – albeit for a highly limited audience. However the intelligence agencies are also becoming involved in crowdsourcing intelligence, for example, one $13M project through US military research body, DARPA, Deep ISR Processing by Crowds, sought to "harness the unique cognitive and creative abilities of large numbers of people to enhance dramatically the knowledge derived from ISR systems." (Drummond 2010).

Even as the NSA's already deliberately lax oversight was tested or bypassed by the agency in the post 9/11 'War on Terror' and the era of Homeland Security, whistleblowers continued to reveal more about the NSA and the wider system of security intelligence. The 2000s saw the emergence of Wikileaks, a new collective effort to provide a public document dump for whistleblowers online, in a more usable, Web 2.0 format than the original Cryptome. The bona fides of some of the new wave of whistleblowers, for example Russell Tice, have been questioned, but attempts to discredit whistleblowers as psychologically damaged, or simply as disgruntled employees, are hallmarks of the way in which intelligence services fight back against those who would seek to reveal their activities. The same thing happened with Wayne Madsen, and is still happening with Edward Snowden, with newspapers close to particular states, like *The Times* of London (e.g. Haynes 2015), printing unsupported claims from unnamed sources that Snowden's revelations have put field agents at risk or given terrorist networks an advantage. Tice was one of the first in the post-9/11 environment to claim that the NSA was, once again, involved in the illegal wiretapping of US citizens.

Tice's claims were however backed and extended by other more high profile whistleblowers like William Binney and Thomas Drake, both of whom were more senior officials in the NSA, concerned by the huge amount of money put into a major NSA program called TRAILBLAZER, which was aimed at the dragnet gathering of internet communications, whose concerns were first widely publicized in the *New York Times* in 2005 (Risen and Lichtblau 2005). Drake's prominence made a prosecution almost inevitable, but all charges except for one minor and largely symbolic indictment were dropped in 2011[2].

Workers from other parts of the Security-Industrial Complex continued to speak out too, the most notable being Mark Klein, a former AT&T technician. He who revealed the extent to which the NSA had infiltrated itself into the American telecommunications network, with a network of parallel exchanges in important telecoms buildings (Klein 2009). These revelations led to Andrew Clement and his team at Toronto's experiments in tracking where data packets go to confirm Klein's information and to identify where the most likely places for as-yet undiscovered NSA exchanges might be[3].

Into this mix, in 2013, stepped Edward Snowden. In many ways, he is exemplary of this strange and contradictory age of surveillance and transparency: far from being a senior internal figure like Drake or Binney, an actual working spy like Madsen or Tice, or even a developer for a technology provider and contractor like Margaret Newsham or Klein, he was simply a systems administrator, one of many recruited on rolling contracts with different private sector contractors for the NSA, in his last assignment for Booz Allen Hamilton – Mike McConnell's outfit. But his position gave him unprecedented accessed inside an agency that was revealed as being networked and insecure to a reasonably well-trained hacker as any other organization in the wider society it monitors. We do not intend to tell his story here. It has been well-documented by Glenn Greenwald in *No Place to Hide* (2014), by Laura Poitras (2014) in *Citizenfour* – the

[2] See court documents at: https://fas.org/sgp/jud/drake/
[3] IX Maps site: https://ixmaps.ca/

two investigative journalists whom Snowden originally approached – and the team from *The Guardian* newspaper, for whom Greenwald was then working, in *The Snowden Files* (Harding 2014). What this two-part issue does instead is to reflect on the implications of the Snowden revelations for surveillance and security intelligence and for surveillance studies.

In this first part, we have 5 articles. In the first, David Lyon, author of a new book surveillance after the Snowden revelations (Lyon 2015), considers what is it stake as a result of the Snowden revelations, noting three type of research responses: firstly, 'research disregard' – the lack of contextualisation of responses to Snowden in the immense amount of research done on surveillance over the last forty years; secondly, 'research deficits', where we are lacking in knowledge; and finally, 'research direction', which Lyon argues means reorienting surveillance research conceptually around the challenges of the Internet. In the second, Miguelángel Verde Garrido reconceptualises the global political economy of surveillance as informed by Snowden and his collaborators in the media. He argues that Snowden's truth-telling practices (*parrhesia*) constitute a kind of "parrhesiastic sousveillance" as "a technologically-enabled modality of resistance" and lead to a genuine digital agency for global civil society. Third, Jason Keiber also considers the wider context of Snowden's revelations, but what he calls the "information ecology made possible by U.S. surveillance hegemony", in other words the way in which other states have understood, normalized and accepted the surveillance practices of the NSA. Lonneke Van der Velden consider the range of data capture technologies implicated in NSA activities, distinguishing between "devices that leak data versus devices that are inserted into computers or networks in order to capture data", arguing for a somewhat different technological research focus than Lyon researchers, on devices that "get close". Finally, Matthias Schulze considers the early reactions to Snowden, in one country in particular, Germany, but presenting "a framework for the study of surveillance legitimizing strategies in scandal discourses that can be used for future cross-case comparisons". He shows that the surveillance legitimizing practices by the German state follow a logic of escalation from several stages of denial through acknowledgement to complaint. These articles constitute only the first part of our After Snowden themed issue, with Part 2 to be published later in 2015.

References

Bamford, J. 1982. *The Puzzle Palace: A Report on America's Most Secret Agency*. New York: Houghton Mifflin.

Bamford, J. 2002. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor.

Bamford, J. 2008. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday.

Bradshaw, J. 2015. How a student secured Edward Snowden for a chat at his high school, *The Globe and Mail*, January 30. http://www.theglobeandmail.com/news/toronto/how-a-student-secured-edward-snowden-for-a-chat-at-his-high-school/article22730776/

Campbell, D. 1984. *The Unsinkable Aircraft Carrier: American Military Power in Britain*, London: Michael Joseph.

Campbell, D.1988. They've Got It Taped, *New Statesman*, August 12, pp.10-12. See: http://www.duncancampbell.org/content/new-statesman-1988

Campbell, D. 1993. *The Hill*, an IPTV Production for Channel Four Television. http://www.duncancampbell.org/content/hill

Campbell, D. 1999. *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: the state of the art in Communications Intelligence (COMINT)* AKA *Interception Capabilities 2000*. Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme. Reprinted at: http://fas.org/irp/eprint/ic2000/ic2000.htm

Campbell, D. and M. Hosenball. 1976. The Eavesdroppers, *Time Out,* June 1976. Reprinted at: http://cryptome.org/jya/echelon-dc.htm

Campbell, D. and L. Melvern. 1980. America's Big Ear on Europe, *New Statesman*, July 18, pp. 10-14. Reprinted at: http://cryptome.org/jya/echelon-dc.htm

CBS. 2000. Ex-Snoop Confirms Echelon Network: Global Network Monitors Phones And Email**,** http://www.cbsnews.com/news/ex-snoop-confirms-echelon-network/ Full transcript at: http://cryptome.org/echelon-60min.htm

Drummond, K. 2010. Darpa's New Plans: Crowdsource Intel, Edit DNA, *Wired* Danger Room Blog, February 2, http://www.wired.com/2010/02/darpas-new-plans-crowdsource-intel-immunize-nets-edit-dna/

Elkjær, B. and K. Seeberg, Kenan. 1999. Echelon Was My Baby, *Ekstra Bladet*, Denmark, November 17. Translated and reprinted at: http://cryptome.org/echelon-baby.htm

Greenwald, G. 2014. *Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Picador.
Hagar, N. 1996. *Secret Power, New Zealand's Role In the International Spy Network. (Second edition)*, Nelson, New Zealand: Craig Potton. Reprinted at: http://www.nickyhager.info/ebook-of-secret-power/
Harding, L. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man.* New York: Vintage.
Hayes, B. 2009. *NeoConOpticon: The EU Security-Industrial Complex*. London: Statewatch / Transnational Institute. http://www.tni.org/report/neoconopticon
Haynes, D. 2015. Full damage of Snowden leaks revealed, *The Times*, March 18. http://www.thetimes.co.uk/tto/news/uk/defence/article4385198.ece
Johnson, L.K. 1988. *A Season of Inquiry: Congress and Intelligence (2nd Edition)*, Chicago: Dorsay.
Klein, M. 2009. *Wiring Up Big Brother – And Fighting It*. BookSurge.
Lyon, D. 2015. *Surveillance After Snowden*. Cambridge: Polity.
Nation Review (1973) Uncle Sam and his 40,000 Snoopers. Reprinted at: http://cryptome.org/jya/nsa-40k.htm
Piodi, F. and I. Mombelli. 2014. *The ECHELON Affair: The EP and the global interception system 1998 – 2002*. European Parliament Directorate-General For Parliamentary Research Services, Historical Archives Unit. Luxembourg: Publications Office of the European Union. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU%282014%29538877
Poitras, L. 2014. *Citizenfour*, https://citizenfourfilm.com/
Ramparts. 1972. U.S. Electronic Espionage: A Memoir, 11(2): 35-50. Reprinted at: http://cryptome.org/jya/nsa-elint.htm
Richelson, J.T. and D. Ball. 1985. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*, London: Allen & Unwin.
Risen, J. and E. Lichtblau. 2005. Bush Lets U.S. Spy on Callers Without Courts, *The New York Times*, December 16. http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html
Robb, J. 2005. The Open-Source War, *New York Times*, October 15. http://www.nytimes.com/2005/10/15/opinion/the-opensource-war.html
Shane, S. and T. Bowman. 1995. No Such Agency, series of 6 articles, *Baltimore Sun*. Part 4 reprinted at: http://cryptome.org/jya/nsa-sun.htm
Singel, R. 2010. Cyberwar Hype Intended to Destroy the Open Internet, *Wired* Threat Level Blog, March 1. http://www.wired.com/threatlevel/2010/03/cyber-war-hype/
Vest, J. and W. Madsen. 1999. A Most Unusual Collection Agency: How the U.S. undid UNSCOM through its empire of electronic ears, *Village Voice*, February 24 - March 2. Reprinted at: http://cryptome.org/jya/nsa-scs.htm
Wood, D. 2001. *The Hidden Geography of Transnational Surveillance: Social and Technological Networks around Signals Intelligence Sites*. Unpublished PhD thesis, University of Newcastle upon Tyne.
Wright, S. 1998. *An Appraisal of the Technologies of Political Control: Interim STOA Report (PE 166.499)*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme. Reprinted at: http://aei.pitt.edu/5538/
Wright, S. 2005. The ECHELON Trail: an illegal vision, *Surveillance & Society* 3(2/3): 198-215. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3501

Resources

Duncan Campbell: http://www.duncancampbell.org/
Cryptome, http://cryptome.org
Electronic Frontier Foundation: https://www.eff.org/
Electronic Privacy Information Centre (EPIC) https://epic.org/
Federation of American Scientists (FAS) http://www.fas.org/irp
Global Security, http://www.globalsecurity.org/
The Guardian 'NSA Files': http://www.theguardian.com/us-news/the-nsa-files
The Intercept https://firstlook.org/theintercept/
National Security Archive (George Washington University) http://nsarchive.gwu.edu/
Der Spiegel Snowden documents: http://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html
Omega Research Foundation: http://omegaresearchfoundation.org/
Privacy International: http://www.privacyinternational.org/
Statewatch: http://www.statewatch.org/
Washington Post 'NSA Secrets': https://www.washingtonpost.com/world/national-security/nsa-secrets/
Wikileaks https://wikileaks.org/