KEY WORDS

ALGORITHMIC SURVEILLANCE; UNEASY ETHICS; RESEARCH ACTIVISM; MEANINGFUL HUMAN CONTROL

ABSTRACT

WATCHING THEM: WATCHING US – WHERE ARE THE ETHICAL BOUNDARIES?

Steve Wright argues that the process of watching official and unofficial surveillance activities, is guided by an "uneasy ethics." It can never be a neutral behaviour since someone is benefitting or being dis-benefitted, from both being watched, or being the watcher. The role of the military, security, police, university, media entertainment, industrial complex is now core. Surveillance capacities are being rapidly expanded, whilst existing checks and balances prove both inadequate or in a state of erosion. What can be done in the face of such change and who will create the requisite reinforcement, the checks and balances to prevent surveillance remorselessly moving even further beyond the limits of the law? Wright argues that this is a core issue of applied ethics: it cannot and should not be a sterile exercise in social and political astronomy; not if constitutional democratic systems as we know them are to survive. He calls for a much wider debate on the notion of meaningful human control…and the crucial roles of both whistleblowing and research activism.

WATCHING THEM: WATCHING US – WHERE ARE THE ETHICAL BOUNDARIES?

Dr Steve Wright: Reader in Applied Global Ethics; Leeds Beckett University

Introduction

A key assumption in this paper is that the process of watching advances, proliferation, procurement and deployment of surveillance, is guided by an 'uneasy ethics.' The term, which was first coined by Professor Simon Lee, marks an effort to grapple with ethical dilemmas that have no universally accepted solutions.(Lee, 2003). Such invidious choices demand intense reflection on what core values are at stake, what is being defended for the sake of what is being sacrificed. It is a very different notion to that of 'elastic ethics,' where moral values are continuously shifted to justify the expedient actions of the time.

What complicates such ethical debates when discussing both security and surveillance, especially mass surveillance, is that many of the practices under scrutiny are secret, guarded in some cases by legal or commercial sanctions, where those with the most knowledge are not allowed to speak. The Leeds University academic, Professor Phil Taylor, before his untimely death in 2010, argued that 'psychological operations' in wars, both old and new, is now a vital ingredient. (Taylor, 2003). Indeed, separating fact from propaganda is an academic requirement in this field, since the arguments on all sides, are usually persuasive and hotly contested. It can never be a neutral behaviour since someone is benefitting or being dis-benefitted, from both being watched, or being the watcher. There are competing agendas - which are more than just about privacy versus security.(See Briant, 2015); (Smith, 2007).

We are all now aware that deliberate deception over security issues has led to some extremely costly errors over the years - none more topical than the decision to invade Iraq? But what has that got to do with Post 9/11 surveillance issues? Well, a key shift has been the transition from a position of counter-terrorism, as a civilian law enforcement practice and process: to the US

led, ‘war on terrorism,’ which has required a massive new global approach to surveillance: military surveillance – or so we are led to believe. The Snowden revelations discussed below evidence the corrosive realities of substituting military for civilian surveillance, especially since the former operates under a different legislative framework and brings together contradictory capacities – essentially, what Dr. Ben Hayes of Statewatch has characterised as ‘armed big brother.’(Hayes, 2006), and Stephen Graham, as ‘armed vision. (Graham, 2010).

Testing this paradigm involves asking some searching questions such as who or what are legitimate targets and where are the boundary conditions and what processes ensure that thresholds are not crossed, because of either technological or decision drift, or short term political expediency? Such boundaries are both quantitative and qualitative. It is not just the quantum jumps in the sheer numbers of those officially targeted for surveillance that create ethical dilemmas; it is also the amalgamation of processing power to interrogate the process of watching. Such factors include memory and contextualization in terms of who the target was and is, in terms of identity, affiliations, form and any suspect proclivities held on file.

This data-veillance dimension is further enhanced by algorithmic capacities: surveillance systems that can be taught (via neural network software), to recognize and hunt specific individuals, their vehicles or even certain forms of behaviour. Increasingly, this intelligent surveillance can operate autonomously, for example in the case of Automatic number plate recognition (ANPR), where speeders can be automatically detected and fined in real time, or the attached database can be used to autonomously search for wanted individuals or vehicles in the flow of mass traffic. This new architecture of continuous surveillance is being further enhanced and extended into the public domain with the advent of increasingly reliable face recognition and spooky, once human traits, such as the ability to learn.

Surveillance, Paranoia And The Rise of Surveillance Studies

Paranoia over government surveillance is almost a modern archetype. What has distinguished academic study of surveillance over recent years is its formation of a body of concepts, practices and the systematic analysis of what else happens when surveillance technologies are deployed in terms of selection, social sorting and less obvious issues such as the 'chill factor' of being watched and what it is to theorize surveillance.(Lyon, 2006) What has emerged is a new discipline – surveillance studies, (Lyon, 2007), which has its own journal, Surveillance & Society, Study Readers and Handbooks, (Hier, & Greenberg 2007) and (Ball, Kirstie, et al. 2012) and an organised network of Scholars – the Surveillance Studies Network (SSN).

But is this academic scrutiny enough to deliver us from what has been characterised as a drift into a 'surveillance society' (House of Commons, 2008)? Well, the academic community have certainly done an excellent job in deconstructing the social and political dimensions of what characterises modern surveillance. We now have organized knowledge on theorizing surveillance(Lyon 2006); surveillance and crime (Coleman & MacCahill, 2011); surveillance as governance, (Deflem, 2008); the movement from evidence to information (Sharpe, 2000); surveillance as profiling and social sorting(Lyon, 2003) surveillance and comparative approaches to crime prevention, (Painter & Tilly, 1999); surveillance as social control (Newburn and Hayman, 2002); privacy of course, (Neyland 2006); detailed work on problems associated with specific areas such as CCTV(Koerner,2014) algorithmic surveillance (Norris & Armstrong., 1999) &.(Introna and Wood,2004); mass telecoms interception (Diffy and Landau,2010), or even novel and emerging new areas of criminality, such as cybercrime (Thomas and Loader, 2000).

A growing concern is that such activities essentially amount to social astronomy: record keeping which merely measures the rapid erosion of privacy rights which were once lingua franca,

without directly influencing the object of concern to any real extent. Of course one of the key roles of the academic community, is to highlight such concerns as privacy, for example via calls for enhanced accountability,(Guagnin, 2012) The surveillance-studies community from its formation has raised issues about its impact on globalisation, (Mathiesen, 1999); democracy (Haggerty and Samatas, 2010) border control, (Zureik and Salter, 2005) and the growing economic and political power of the security, industrial complex.(Hayes,2010 ; Ball and Snider, 2013).

The European Commission under the FP7 funding programme has funded research programmes which depth-charge the societal and ethical impacts of the relentless pace of change in surveillance technologies and capacities. (E.g. projects such as PACT, which facilitated "citizens perspectives on surveillance' through a survey of 26,000 participants to explore 'controversies, alternatives and solutions, (http://www.projectpact.eu/) and SECILE, which examined the 'impact, legitimacy and effectiveness of counter-terror measures' including surveillance, (http://cordis.europa.eu/project/rcn/108566_en.html). Within the UK, the ESRC has also funded perceptive multi-disciplinary programmes of academic inquiry into surveillance, such as the ongoing DATA-PSST! Seminar project which has organised a useful debating forum. (http://data-psst.bangor.ac.uk/)

But whilst these initiatives are welcome and provide an important early warning system about the negative and unforeseen impacts which may emerge: measurable, direct impacts of academic work on burgeoning surveillance practices and processes are difficulty to ascertain. Certainly, academics can inform future policy but paradoxically it can be the process of ethics approval itself which can be the major obstacle, since few universities condone research which is directly confrontational or risks significant legal problems or potential commercial challenges over loss of income.

If we are searching for high impacting initiatives in regard to countering untoward surveillance, it is necessary to focus on the activities of NGO's, whistle-blowers and media. Such groups are more interested in applied ethics and are focussed on results rather than publications, milestones and esteem factors, important and present though they may be. Increasingly, however, academics are working with NGO networks to create a spine of research-based activism. Such amalgamated networks especially with media-savvy activists and campaign groups can provoke formidable challenges[1]. (See below)

Some Historic Trends in Surveillance Activities and Capacities[2]

These shifts in the official capacity to gaze, now operate within a 'veillance' or 'mutual surveillance 'environment, of them watching us watching them; albeit with vastly asymmetric resources of finance, capability and relentlessness. To ethically judge this asymmetry, it is worth analysing some of the historic data on monitoring trends and their implications. Whilst the need for surveillance in modern times is consistently presented as a pre-requisite for efficient crime control and effective counter-terror ops, historically it is a practice long associated with maintaining public order and political control.

Long before it becomes necessary to directly intervene in street level politics, most nation states, even liberal democratic ones, take steps to assess and monitor the activities of their opposition. There is nothing new in this. The British state has a long history of covert surveillance of the public, which predates the setting up of the Special Branch in 1883. The Elizabethan Court ran a massive network of government informers and spys. The 1838-48 Chartist struggle for a

[1] An example at the time of writing, is the Amnesty Video campaign against an arms fair taking place in central London, where advanced surveillance technologies were on show. It had already been viewed over 100,000 times after 1 day and was accompanied by an illegal fly posting of spoof adverts on the London Underground. http://www.theguardian.com/world/shortcuts/2015/sep/16/illegal-torture-equipment-on-doorstep-adverts-shaming-britains-arms-trade?CMP=Share_AndroidApp_Email

[2] The section draws from Wright, (1987).

widening of the franchise, also witnessed country-wide surveillance through paid informants and spies. What has changed, is the sheer capacity for state-monitoring of the populace, provided by the new technologies. But do sheer increased numbers make the surveillance issue more ethically problematic? Or is it the shifting mesh of just who can become caught up in the observational net and the level and extent of other factors that can be brought into that gaze, regardless of innocence or guilt? Professional, centralised government control, has morphed into a ubiquitous but largely invisible surveillance presence. But what are the boundary conditions which will persuade us that the surveillance revolution has become unethical, that some critical threshold has been passed?

We know from human centred mass surveillance networks, like that run by the Stasi, in former East Germany, that untrammelled police surveillance can insidiously lead to an authoritarian society under mass supervision. But could we establish critical ethical thresholds for modern surveillance networks, given that they have moved on from 1-1 surveillance, to 1-many?

Such transitions are governed by changes in three key dimensions, namely:-

- (i) Rapid innovation in surveillance technology which significantly enhances police ability to scrutinize large sections of the populace, unobtrusively, day or night, both visually and electronically, by direct monitoring or geo-location means, remote from the watching zone;
- (ii) Changes in the structure, identity and function of the operational units allowed to undertaking this watching role, with an overall imperative towards autonomous operation with learning function which enhance surveillance faculties over time;
- (iii) The erosion of police and intelligence agency accountability and constitutional protections for ordinary citizens, who not infrequently, may have their right to privacy illegitimately and illegally overridden, or totally ignored.

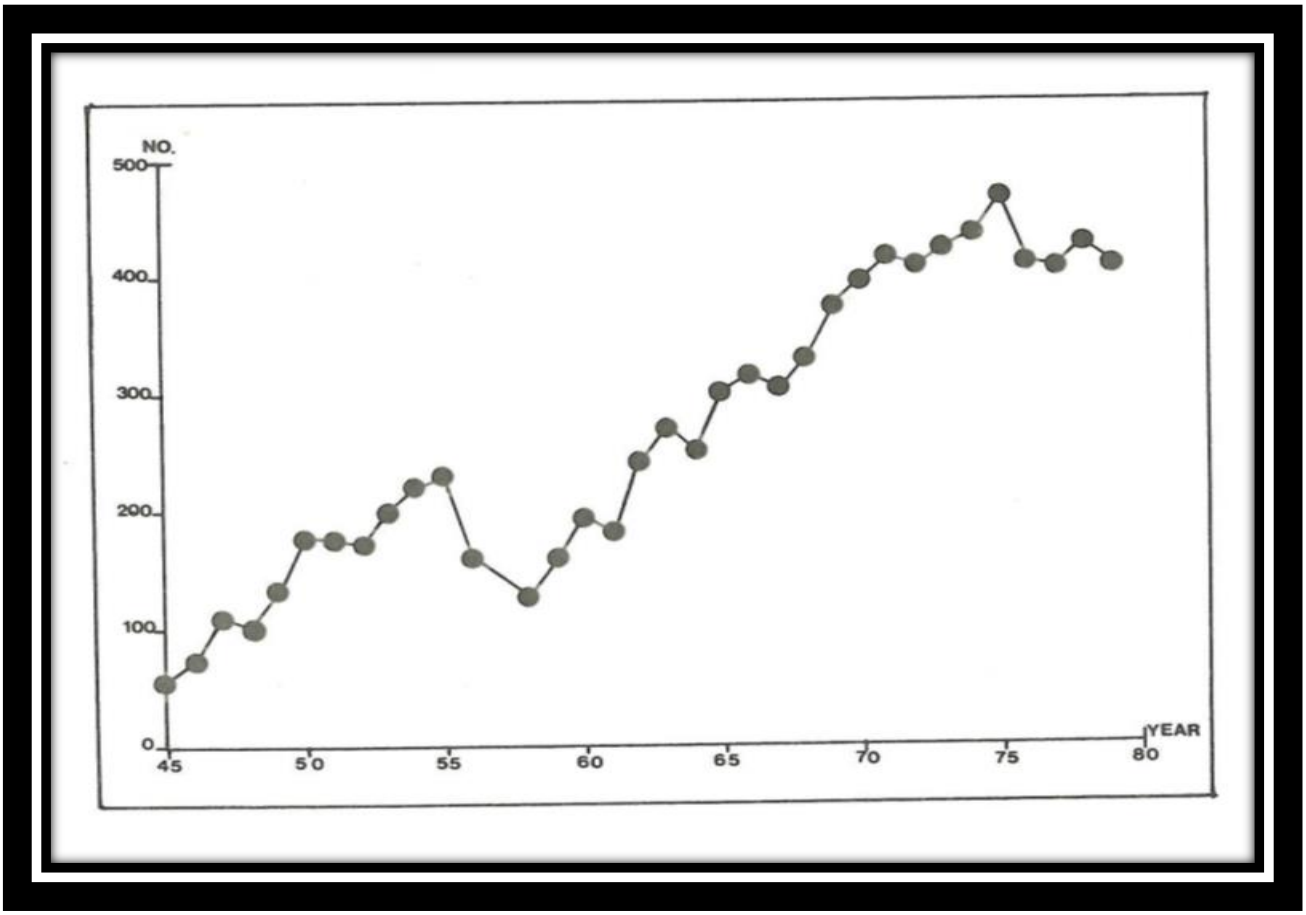
FIG 1. STATISTICS ON INTERCEPTION U FROM 1937- 1979 (Wright, 1987)

YEAR	TELEPHONES	LETTERS	TOTAL
1937	17	335	352
1938	20	422	442
1939	29	643	672
1940	125	1,192	1,317
1941	180	833	1,013
1942	164	512	676
1943	126	327	453
1944	102	213	315
1945	56	90	146
1946	73	139	212
1947	110	162	272
1948	103	156	259
1949	133	183	316
1950	179	232	411
1951	177	261	438
1952	173	237	410
1953	202	240	442
1954	222	223	445
1955	231	205	436
1956	159	183	342
1958	129	109	238
1959	159	101	260
1960	195	110	305
1961	183	75	258
1962	242	96	338
1963	270	128	398
1964	253	120	373
1965	299	93	382
1966	318	139	457
1967	307	92	399
1968	333	83	416
1969	377	93	470
1970	395	104	499
1971	418	86	504
1972	413	95	508
1973	424	73	497
1974	436	93	529
1975	468	93	561
1976	410	62	472
1977	407	84	491
1978	428	44	472
1979	411	52	463

NOTE: The figures from 1946-1955 are taken from the 'Birkett Report', (Cmnd. 283,1957). Figures for Home Secretary warrants from 1958 -1979, are taken from 'The Interception of Communications in Great Britain',(Cmnd. 7873, 1980). All statistics are distinct from those covering Scotland which are presented seperately.

The growth of surveillance in the UK can be traced back to the 1950's. In 1957, when Lord Birkett produced the first official report on telephone interception in the UK, telephone tapping was very much a cottage industry, (HMSO,1957).Since then, telephone interception has grown into today's sophisticated high capacity, space- satellite based hi-tech systems. Nevertheless, when these figures were officially updated in 1980, many MP's were surprised by the relatively modest official increase over the intervening 23 years.. That is from 129 warrants in 1958, to 411 warrants in 1979, for England and Wales. (See Fig 1 & 2).

FIG. 2 HOME SECRETARY TELEPHONE WARRANTS ISSUES (1945-1980)



However, the 1980 White paper on the Interception of Communications did admit that one warrant could cover multiple intercepts of any organisation, and its entire membership,, e.g. CND. (HMSO,1980). It was also revealed that the Secretary of State 'may delegate' to the civil

service, the power to amend a warrant. Thus the total number of lines monitored is likely to be substantially more than the absolute number of warrants issued.

Another anomaly was revealed when Clement Freud MP asked, 'whether the number of interception orders is cumulative, that is to say, those currently in force – or is the number given simply that of the new orders that have been published?' The then Home Secretary, William Whitelaw, refused to answer, leaving open the possibility that key permanent warrants for MI5 & Special Branch, are merely issued once. (Campbell, 1981)

Other law enforcement surveillance during this era, especially visual surveillance was often politically focussed, without much evidence of ethical reflection. Illustrative examples include operations setting up cameras in a Tyneside Factory[3]; police TV cameras hidden in a false jukebox loudspeaker, in a pub in Hartlepool[4]; Kent police setting up hidden cameras in toilets, sports clubs and car parks[5]; two way mirrors used by Special branch to observe the 1978 T.U.C. conference[6]; the bugging of a Welsh telephone box in Tal-y-Sarn[7]; the planting of \vehicle tracking bugs in London[8]; the setting up of spy posts to watch gay pubs(Cox & Scott, 1984) and black communities in Manchester[9]; the Metropolitan police takeover of the London Traffic CCTV system (CITRAC), for public order surveillance operations[10]; and extensive Special Branch bugging of CND and the peace movements.[11]

But whist the justification of such snooping was ethically justified by reference to international threats and the 'enemy within', the figures don't bear this out. For example.it might be supposed

[3] Daily Mail,20.2.1981
[4] The Mirror, 28.9.1979
[5] Rampet Bulletin, November, 1985
[6] Socialist Worker, 16.10.1978
[7] Guardian 13.1.1982 and 11.2.1982
[8] New Statesman 21.6.85 and 5.7.85
[9] Manchester City Council Police Monitoring Reports, 27.10.1986 & 1.12.1986
[10] Rampet op.cit
[11] See former MI5 operative Cathy Massiter's interview on Channel 4's 20/20 Vision's 'M I5's Official secrets', February, 1985. Further background is provided in (Reeve & Smith, 1986)

that the development of international terrorism in the early 1970's had fed the growth of telephone surveillance. However, the trends in Figs. (1 & 2) tell a different story. The sharp boom in UK telephone tapping came immediately after Birkett, who recommended that in future, official figures on tapping should not be made public. The growth period occurred during the 1960's, before international terrorism, (the ostensible reason given in the 1980's for increasing official surveillance), became a major problem. If anything, the rise in the growth of surveillance slackened in the 1970's, just as domestic terrorism in Northern Ireland, had become an acute problem. And here we have the rub, the White papers did not cover Northern Ireland, nor did they mention tapping warrants signed by the Foreign Secretary for GCHQ and the SIS, nor interception warrants signed personally by the Prime Minister.. These were important omissions, given that in 1967, one permanent warrant authorized GCHQ to intercept all foreign telegrams.[12]

And yet, by modern standards, the scale of these operations is relatively small, though it did not seem so at the time. This was despite the fact that this period covered the height of the Cold War and in the 1970's, there were between 366 and 1382 bomb explosions a year, in Northern Ireland. (Wright, 1987).

So what changed since? Well, in the 1980's, we rapidly moved from an analogue to a digital world. In practical terms that meant processing capacities which delivered new capabilities which facilitated new ways of thinking about how searches can be conducted. Breakthroughs in technology enabled new tools for mass surveillance, using sophisticated computation, algorithmic programs and artificial intelligence: neural networks which enabled searching flows of information for designated anomalous, aberrant behaviour, rather than for specific individuals. All this was accomplished without much reflection on legal, or ethical dimension, or even a recognition that emergent practices required some new forms of ethical oversight and

[12] As part of the Minaret programme, under the 1947 UKUSA pact – revealed in (Bamford, 1983)

accountability. In Manchester, in 1984, the Chief Constable saw fit to carry out surveillance of his own officers telephone calls, in a moral panic about whether or not they were having affairs. (Lashmar, 1984). Such cases raised a sense of righteous indignation, since if the police were not immune against unauthorised surveillance, who was?

The period saw a surveillance revolution, with the Association of Police Chief Officers (ACPO) playing a pivotal role, especially during the Miners' Strike, where automated number plate recognition(ANPR), was introduced for the first time, leading to arrests of travelling pickets on access roads, long distances away from their strike actions. Today, ANPR covers much of the UK's major trunk roads and motorways. By April 2012, the database held over 11.2 billion vehicle sightings. This led it to be characterised as the" biggest mass surveillance system no one has ever heard of" and prompted the Government's Surveillance Commissioner, Tony Porter to call for new guidelines.[13]

But this nationalization of ANPR was not the only mass proliferation of visual surveillance capacities in the UK. The total number of CCTV cameras grew exponentially from a handful in the 1960's, to a current, but contested estimate of 4.3 million, in the new millennium, (McCahill and Norris, 2002). Why so many British cameras, when Denmark outlawed them with no dramatic discernible differences in crime prevention and control? Well the 'drivers' in the UK were complex but essentially not evidence-based or greatly inconvenienced by deep ethical debate. Much has been written by criminologists about the patchy effectiveness of CCTV (Ditton & Short, 1999; Farrington et. al., 2007; Gill et. al., 2007) and the Home Office made sterling efforts to produce an objective evaluation of their impact (Gill & Spriggs, 2005)). But it was a technology which as one writer had it, crept under the radar. (Koerner, 2014) Why was the

[13] http://www.independent.co.uk/news/uk/home-news/privacy-in-peril-vast-network-of-roadside-cameras-pose-very-real-risk-says-surveillance-regulator-9270377.html

UK so pre-eminent in pioneering this form of surveillance? Were there any significant or critical turning points or insights into processes relevant to other forms of surveillance innovation, which rapidly proliferate without deep ethical scrutiny?

The historical narrative tells us that it was a complex case of many local authorities urgently requiring visible crime prevention measures, coupled with the City Challenge initiative where government ran a competition between 1994 and 1999 for a slice of capital grants worth £38.5 million. The process of selection was competitive and based on wider focussed call for crime prevention partnerships. This not only resulted which resulted in 585 CCTV schemes being set up nationwide, but also a more intense professionalization of the procurement process (Home Office, 2007). This move towards a deeper institutionalization of CCTV, was further catalysed by the tragic murder in Liverpool of toddler James Bulger, with his murderers captured on CCTV, in February 1993. It proved a turning point in public acceptance of greater numbers of sophisticated CCTV cameras,

The R&D costs for this expensive technological innovation were originally covered by Defence expenditure for the Vietnam War and such military genesis influenced its urban configurations.

Further proliferation saw such cameras being integrated into military style communication, command and control centres, built by the same defence contractors. In effect, they created innovative surveillance architectures and networks, into which other surveillance systems could be plugged in….and they were. New methods of crime control and mass supervision such as electronic tagging could now be run on the telecommunications backbone provided by the mobile phone national aerial network.(Paterson, 2007) Some argued this shifting capacity in surveillance technology represented the emergence of a new technology of political control, (Wright, 1998). Others, such as Prof. Edward Halpin, have suggested at a deeper level, it marks the bureaucratic capture of the governance narrative of how acceptable modern crime control

technologies are defined, in policy agendas and processes. Essentially this sleight of hand works by incentivizing monetized techno-fixes over less costly options, devoted to increased community cohesion rather than surveillance. [14]

The outcomes in terms of crime control, may be inconsistent and even contradictory, but the rise and rise of the surveillance industry has been exceptionally lucrative, as this urban supervision model proliferates, both internally and internationally. For example industry sources suggest that more than 17 thousand cameras have recently been installed in Chicago and a whopping 400,000 in Beijing, (70 thousand of which have been installed since 2010).[15]

Of course this technology is not neutral. Its architecture enables real time processes of mass supervision that allow other dimensions of the target subject to be focussed on automatically and sometimes autonomously and its increasing integration into web-based systems allows a new magnitude of sorting and focus, Nowhere is that more significant than with the shifts in capacity for telecommunications interception, discussed earlier. Increasingly, the limits to its capacity are not set by ethical debate but by political and technological persuasion, much of which has remained hidden from public gaze.

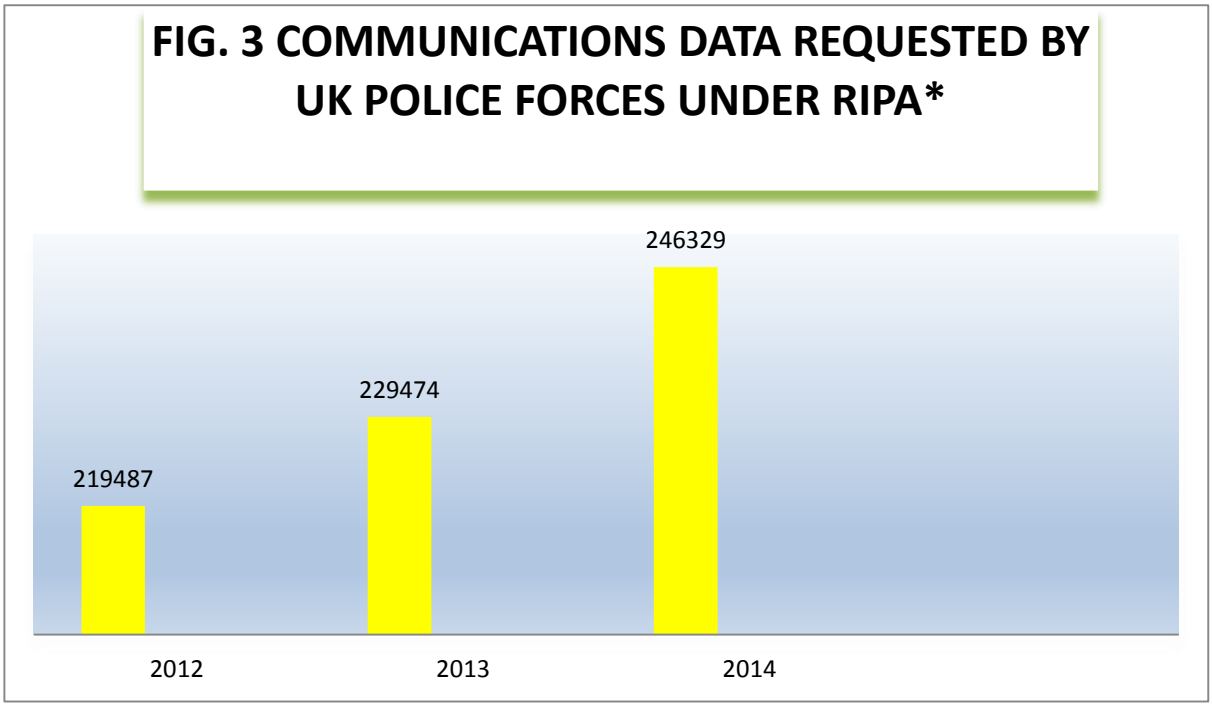
Data revealing the changes in magnitude in official interceptions has recently been compiled by

Tony Bunyan at Statewatch. These indicate a jump in phone tapping warrants and mail opening from 1712 in 1997, to 18,612 in 2012. But the techtonic shift in UK surveillance activity is revealed by requests for access to communications data (which covers not only phone calls, but email, fax, mobile phone and location and internet usage. Statewatch records that these annual interceptions have jumped from 351,243 in 2005/6 to 517,236 in 2014. (Bunyan, 2015)

[14] In conversation with the author, September 2015.

[15] http://www.vintechnology.com/journal/uncategorized/top-5-cities-with-the-largest-surveillance-camera-networks/

The NGO, Big Brother Watch (BBW) has suggested that a 'new normal' has emerged. Between 2012-2014, UK Police Forces made 733,237 requests for Communications data (See Fig 3), with a refusal rate of only 4%. BBW say this is equivalent of 670 requests a day or 28 requests every hour. (Big Brother Watch, 2015) Such figures question the notion of effective and ethical oversight of what is a highly and intrusive activity and suggest we have moved into an era of virtually automatic approvals.



Data taken from Big Brother Watch (2015) – Police Access to Communications Data: How UK Police Forces request Access to Communications 700,000 times in 3 years.

But even those figures which evidence a vast change in UK police surveillance praxis, are dwarfed by warrantless communication interception activities associated with the intelligence agencies, especially America's world-wide National Security Agency (NSA) and its junior UK partner, GCHQ.

It is now fashionable to associate the rapid rise of surveillance with the security demands of a post 9/11 world and consciousness of what the authorities have to do in our name, with the revelations of Edward Snowden (Greenwald, 2014). Such demand pull scenarios might be more correctly viewed as legitimations. Certainly post 9/11, expenditure increased massively and post 7/7 London bombings MI5 doubled in size. However, the role of technology push in creating unprecedented surveillance capacity is now historically evidenced by Hager (1996) and more publically by work undertaken for the European Parliament by Wright (1998) for the Omega Foundation; Campbell (1999) and others, on the dictionary based autonomous NSA/GCHQ system known as Echelon. Campbell revealed the jump from terrestrial into space based interceptions via Rhyolite (later Aquacade) satellite programmes, from 1967-1985. This technology leap provided gargantuan capacity which has had to be justified both politically and strategically, now the cold war has ended. Campbell warned of the danger of blurring the boundaries between law enforcement and intelligence led interception.[16] The new capability set made prodigious levels of interception possible: 2 million calls per hour was one estimate by (Campbell, 1998), Campbell says the scale of NSA operations has now doubled in scale since 2000,[17] and based on the revelations of Edward Snowden could quadruple in the future.

[16] 'It should be noted that technically, legally and organisationally, law enforcement requirements for communications interception differ fundamentally from communications intelligence. Law enforcement agencies (LEAs) will normally wish to intercept a specific line or group of lines, and must normally justify their requests to a judicial or administrative authority before proceeding. In contract, Comint agencies conduct broad international communications "trawling" activities, and operate under general warrants. Such operations do not require or even suppose that the parties they intercept are criminals. Such distinctions are vital to civil liberty, but risk being eroded it the boundaries between law enforcement and communications intelligence interception becomes blurred in future.' (Campbell, 1999)

[17] According to Campbell, the expansion has been further enhanced by linking in other FORNSAT (foreign satellite) interception sites run by NSA's allies in secret pacts, including Germany, France, Spain, Sweden and Denmark, http://www.duncancampbell.org/

Ethics & Research Activism – The Key Role Of NGO's & Whistle-Blowers

The rapid spread of surveillance capacity has been accelerated by the construction of military communications, command and control architecture, which is an integral part of both the web and the electronic nervous system, which services it on land, sea, air and space. But few question what impact that military dimension has on changing the nature and accountability of the relationships between those who watch and those who are watched. But they are real and insidious, whilst remaining ubiquitous but invisible.

Applying ethical criteria to explore what can be done in the face of such change, involves asking who will create the requisite reinforcement, the checks and balances to prevent new forms of surveillance remorselessly moving beyond the limits of the law? The media, academics, government, or NGO's all have different agendas and limitations. Success or failure by one, may draw fire from the other.

There are some tough critical questions. What role does research have in deconstructing the new surveillance paradigms and their targets? What are the roles and acceptable practices of activists in challenging excess? What are the unanticipated consequences of giving all of our data up to the military who are ritually and ideologically bound to targets, rather the wider concerns of freedom, democracy & justice.

As surveillance capacities proliferate through the global international security markets, not all operators will use that capacity in a democratic way. This will become increasingly important as the targeting capacities built into our security and communications architectures facilitate selective and potentially extrajudicial actions, as weapons, targeting algorithms and surveillance are amalgamated. Urban geographers such as Professor Stephen Graham, were amongst the first academics to recognize the significance of this move away from conventional battlefields, towards a more ubiquitous digitalization and securitization of all urban spaces. This new digital

mapping architecture has transformed all modern cities into so called urban 'battlespaces.' Now, every location can be bulls-eye targeted for both surveillance and potential elimination, using geographic location via mobile phones and unmanned but armed UAV's, or drones. (Graham, 2010). It might be argued that the role of academic researchers in this field is to clarify any societal and ethical implication of such new capacities and provide an early warning if undesirable second and third order impacts emerge. In practice that has rarely happened: it has usually come down to activists, whistle-blowers, leakers and NGO's, to highlight potential anomalies between surveillance security claims, theory and praxis.

NSA have always known that its activities breached privacy and anti- espionage laws, especially in Europe where post WWII, several states had explicit constitutional protections against illicit phone tapping. So where are the real ethical boundaries if transnational surveillance activities breach constitutional norms, both for the agencies involved and for individuals and groups which expose them? Essentially these have to be tested by the systems criteria offered by the Cybernetician Stafford Beer who simplified it thus: "A system is what a system does."(Beer, 2003) That does not mean what proponents of that system argue it does but what the values ensconced in the behaviour actually do.

Like the officially sanctioned process of torture, mass spying is conducted in great secrecy, deniability and grave sanctions await for anyone breaching the code of secrecy surrounding the mal-practice. Like paedophilia in the Catholic Church, the initial response to any accusation is a closing of ranks and a concerted campaign of deniability and obfuscation. So what had and does happen when a suspicion arises, that surveillance capacities and activities emerge which represent not just a new paradigm of intrusiveness, but also present evidence of illegal or politically damaging behaviour? What happens when a single individual or group of researchers decide, up with that I shall not put?

Some of the case examples over the last forty years have involved both field and academic research to expose cover up and collusion with such practices. A key challenge for any such whistle-blowers, is who can you call, who will protect you once you have an agencies guilty little or not so little secrets? What is the ethical thing to do – to whistle-blow or to leak? NGO's and whistle-blowers cover both strands of what might be called research activism but both are built on the notion that the gathering of organised knowledge is sufficient to expose a previous official construction, as an outright lie or dissembling.

In the UK, the ABC trial[18]; The Menwith Hill Women's Peace Camps which used field research from waste bins on site to reveal NSA interception configurations and were used by Campbell[19]; the early networking of researchers into the 'Architecture of Surveillance' via meetings such as "Researching State Structures" (Bledowska, 1983) are cases in point. The STOA Echelon Affaire (Piodi & Mombelli, 2014) and its rebranding and re-empowering of previous research published by Duncan Campbell and Nicky Hager created the pre-requisite 'Ethical Unease.' But at the time in the late 1990's, the European parliament was more interested in Echelon being used for industrial espionage rather than an industrial level invasion of privacy. So creating ethical change means creating a 'critical mass' especially in the written and broadcast media. Revelations about NSA's global surveillance had been known for over two decades, before Edward Snowden in 2013, leaked NSA's own internal documents.

What Snowden's leaks did was perform an intentional political jiu jitsu. Using the ethics of so called "backfire" processes to alert a greedy media, Snowden and his media advisers were able

[18] http://www.duncancampbell.org/content/biography#theabctrail

[19] See Ch4 Dispatches programme – The Hill http://www.duncancampbell.org/content/hill

to project their construction of new security paradigm which falsified many of the alleged factual and ethical claims of the old construction for popular consumption. [20]

Thus we were told that such global surveillance was justified in terms of post 9/11 antiterrorist programmes and so it is. But why, the media asked is the NSA spying on its allies[21]; spying on EU commercial activities (Campbell, 1998) Greenwald, 2014) and NGO's like Amnesty and World Council of Churches, (Wright, 1998); the G20 summits.[22] What alarmed ordinary people as well as foreign politicians and media, was the sheer scale of the intrusion and the fact that social media sites on the internet had provided access to everyone's email and communications.[23]

The numbers were beyond imagining and credible because the documents Snowden revealed were directly from the source and named their programme code words, like PRISM,TEMPORA. GCHQ was capable of intercepting 192 times the capacity of the British lending Library, every single day.[24]

Lord Facolner, former Lord Chancellor of Great Britain, said leaks highlighted the problems of "bulk surveillance and questioned whether surveillance had gone too far when it was revealed that 850,000 people had official access to files leaked by Snowden. Falconer questioned whether the oversight mechanisms were 'fit for purpose.'[25]

What has emerged is an ethical unease about who is *not* a target and what is being done with all the material intercepted? These fears have been compounded when details of the 'Optic Nerve

---

[20] See work of Brian Martin, http://www.bmartin.cc/pubs/backfire.html

[21] http://www.duncancampbell.org/content/embassy-spying

[22] http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

[23] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[24] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[25] http://www.theguardian.com/world/2013/nov/17/threat-nsa-leaks-snowden-files

programme emerged, suggesting imagery including sex texting was being stored and that face recognition programmes were being tested to hunt for persons who might be of future interest.[26]

CONCLUSION: RESEARCH NETWORKS & HEURISTIC LEARNING

Yet the final ethical boundary has yet to be crossed – how do we ensure that people actually care about mass surveillance, since the revelations have stirred up very limited action in the UK and this has been limited to a few newspapers like the Guardian or NGO's such as Privacy International and the Bureau of Investigative Journalists?

NGO's have consistently challenged excesses of surveillance, whether it is LGIU bringing in regulations for CCTV users[27]; creating NGO networks against illegal exports of surveillance technology[28]; or bringing together the legal expertise to successfully challenge NSA spying activity under EU legislation, as did Privacy International.[29] Of course the biggest ethical quandary of mass surveillance has itself received very little media or academic treatment:

What use is all that information surveillance, sex texting interception been put to? We know that the NSA has just built the largest data storage capacity in human history in Utah,[30] so the issue is not going to go away. Only 5% of Snowden's revelations have been made public – once we get to the rest, just maybe a new ethical call for control of surveillance will emerge?

---

[26] http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

[27] http://www.lgiu.org.uk/wp-content/uploads/2012/11/Surveillance-local-authority-powers-are-changing.pdf

[28] https://www.amnesty.org/en/latest/news/2014/04/questions-and-answers-coalition-against-unlawful-surveillance-exports-cause/

[29] https://www.privacyinternational.org/?q=news

[30] http://www.wired.com/2012/03/ff_nsadatacenter/

But the backdrop of media debate creates a context of insecurity which feeds into the notion that ever more intrusive surveillance will be required – a theme which the desperate head of MI5, Andrew Parker, recently made on BBC Radio 4.[31]

Such siren calls are difficult to challenge since they are often made in the midst of ongoing moral panics. What is required is a sober analysis and call for account made when any new surveillance process, technology, or power, is being advocated, especially by groups with deep political and financial vested interests. Progress towards that goal has been made for example in the EU where every new piece of security research commissioned must now have a proper ethical and societal impact assessment.[32] In the longer term we need to be learning and teaching about how society can effectively make its security technologies serve designated and accountable ends, without them corroding the very values they have been put in place to protect. The challenge to the academic and policy communities is to promote alternative and more ethical forms of governance which facilitate such values as a longer term legacy.

....

BIBLIOGRAPHY

Ball, Kirstie, Haggerty, Kevin, & Lyon, David (2012) *Routledge Handbook Of Surveillance Studies*, London : Routledge.

Ball, Kirstie, & Snider, Laureen (2013), *The Surveillance-Industrial Complex: A Political Economy Of Surveillance*, London : Routledge.

Bamford, James (1983) The *Puzzle Palace*, London, Sidgewick & Jackson.

[31] http://www.theguardian.com/world/2015/sep/17/mi5-chief-calls-for-more-up-to-date-surveillance-powers

[32] http://file.prio.no/Publication_files/Prio/Burgess-Societal-Impact-Policy-Brief-9-2012.pdf

Beer, Stafford (2003) *Diagnozing the Sytsem for Organisations*, Chichester, UK, John Wiley.

Big Brother Watch (2015) *Police Access to Communications Data – How UK Police Forces requested access to communications data over 700, 000 times in 3 years*, London, Big Brother Watch. http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/05/Big-Brother-Watch-Report-Police-Communications-Data1.pdf (Accessed 23rd. September 2015)

Bledowska, Celina (1983) *War & Order – Researching State Structures*, London, Junction Books.

Briant, Emma (2015) *Propaganda and Counterterrorism: Strategies for Global Change*, Manchester, Manchester University Press.

Bunyan, Tony (2015) *UK:Surveillance statistics: 1937-2015*, London, Statewatch, March 13. http://www.statewatch.org/uk-tel-tap-reports.htm

Campbell, Duncan, (1981) *Phone Tappers & The Security State*, Report No. 2, London, New Statesman.

Campbell, Duncan (1998) 'Tip for Tap' *The Guardian*, London, 10 September

Campbell, Duncan (1999) *Interception Capabilities 2000*, Brussels, European Parliament, 2000. http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

Campbell, Duncan (2015a) *GCHQ & Me – My Life Unmasking British Eavesdroppers*, The Intercept, https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/ accesed 27 September 2015

Campbell, Duncan (2015b) http://www.duncancampbell.org/PDF/nautilus%20report.pdf

Coleman, Roy & McCahill,, Michael (2011), *Surveillance & Crime*.: London : SAGE.

Cox, Gabriella & Scott, David, (1984) "*Gotcha" – A case study of covert police surveillance*, Manchester, Youth Development Trust..

Deflem, Mathieu (2008), *Surveillance And Governance. : Crime Control And Beyond*.: Bingley, UK: Emerald/JAI.

Diffie, Wilf, & Landau, Susan, (2010) *Privacy On The Line : The Politics Of Wiretapping And Encryption*, Cambridge, Mass; London : MIT Press.

Ditton, Jason. and Short, Emma. (1999), 'Yes, It Works, No, It Doesn't: Comparing the Effects of Open CCTV in Two Adjacent Scottish Town Centres,' in Painter, K. and Tilley, N.(1999).

Farrington, David. P., Gill, Martin., Waples, Sam. and Argomaniz, Javier. (2007) 'The effects of closed-circuit television on crime, meta-analysis of an English national quasi-experimental multi-site evaluation', *Journal of Experimental Criminology*, 3: 21-38.

Gill, Martin. and Spriggs, Angela (2005) *Assessing the Impact of CCTV*, Home Office Research Study 292. London: Home Office.

Gill, Martin., Bryan, Jayne and Allen, Jenna (2007) 'Public perceptions of CCTV in residential area: "It is not as good as we thought it would be', *International Criminal Justice Review*, 17: 304-324..

Graham, Stephen (2010) *Cities Under Siege - The New Military Urbanism*, London, Verso..

Greenwald, Glen (2014) *No Place To Hide : Edward Snowden, The NSA, And The U.S. Surveillance State*, n.p.: New York, New York : Metropolitan Books/Henry Holt.

Guagnin, Daniel , (2012) *Managing Privacy Through Accountability. [Electronic Resource]*, n.p.: Basingstoke; New York : Palgrave Macmillan.

Hager, Nicky (1996) *Secret Power: New Zealand's Role in the International Spy Network*, Nelson, New Zealand, Craig Potton, , http://www.nickyhager.info/Secret_Power.pdf

Hayes, Ben (2006) *Arming Big Brother – The EU's Security Research programme*, London/Amsterdam:Statewatch/Transnational Institute(TNI). *www.statewatch.org/analyses/bigbrother.pdf* (Accessed September 10, 2015)

Hayes, Ben (2010) *Neoconopticon – The EU Security Industrial Complex* London/Amsterdam: Statewatch/Transnational Institute(TNI). http://www.statewatch.org/analyses/neoconopticon-report.pdf (accessed 16 September 2015)

Haggerty, Kevin, & Samatas, Minas (2010) *Surveillance And Democracy*, Abingdon : Routledge.

Hier, Sean P, & Greenberg, Josh (2007) *The Surveillance Studies Reader*, Maidenhead : Open University Press.

Home office, (2007) *National CCTV Strategy, October*, London, *HMSO*

HMSO, (1957) *Report of the Committee of Privacy Councillors appointed to Inquire into the Interception of Communications*, (The Birkett report), London, Cmnd 283.

HMSO, (1980) *The Interception of Communications in Great Britain*, London, Cmnd 7873.

House of Commons – Home Affairs Committee (2008) *A Surveillance Society – Fifth report of Session, 2007-2008*, Vol 1, London, the Stationary office.

Introna, ,Lucas D. and Wood, David, M., (2004) *Picturing Algorithmic Surveillance: The Politics of Facial recognition Systems*, Surveillance & Society, 2(2/3), 177-198, http://surveillance-and-society.org/articles2(2)/algorithmic.pdf (Accessed 14 September 2015)

Kroener, Inga (2014) *CCTV. : A Technology Under The Radar?*: Farnham ,Ashgate.

Lashmar, Paul, (1984) Has Big Brother Got an eye On the Police?,*The Observer*, London.

Lee, Simon (2003) *Uneasy Ethics*, London, Pimlico.

Lyon, David (2003), *Surveillance As Social Sorting : Privacy, Risk, And Digital Discrimination*,: London : Routledge.

Lyon, David (2006) *Theorizing Surveillance: The Panopticon And Beyond*, Cullom Bepton : Willan.

Lyon, David (2007), *Surveillance Studies: An Overview*, n.p.: Cambridge ; Malden, MA Open University Press.

Mathiesen, Thomas, (1999) *On Globalisation Of Control : Towards An Integrated Surveillance System In Europe*, London : Statewatch.

McCahill,, Michael & Norris, Clive (2002) *CCTV in Britain* Urbaneye, *On the Threshold to Urban Panopticon*, Working Paper no. 3. Centre for technology and Society, Berlin, Technical University of Berlin, Germany . http://www.urbaneye.net/results/ue_wp3.pdf, accessed 24 September, 2015.

Murakami-Wood, David & Wright, Steve (2015) Before 7 After Sniowden, *Surveillance & Society*, 13(2):pp. 1-7

Neyland, David 2006, *Privacy, Surveillance And Public Trust*, n.p.: Basingstoke : Palgrave Macmillan.

Newburn, Tim, & Hayman, Stephanie (2002) *Policing, Surveillance And Social Control : CCTV And Police Monitoring Of Suspects*, Cullompton, Willan,

Norris, Clive, & Armstrong, Gary (1999), *The Maximum Surveillance Society : The Rise Of CCTV*, Oxford, Berg,.

Painter, Kate, & Tilley, Nick (1999), *Surveillance Of Public Space : CCTV, Street Lighting And Crime Prevention*: Monsey, N.Y. : Criminal Justice.

Paterson, Craig (2007) Street Level Surveillance, Human Agency and the Electronic Monitoring of Offenders, *Surveillance and Society*, Surveillance & criminal Justice, Part 2, 4(4):314-328

http://www.surveillance-and-society.org/articles4(3)/streetlevel.pdf (accessed, 24 September 2015)

Piodi, Franco and Mombelli, Iolanda, (2014) *The Echelon Affaire – The EP and Global interception system 1998-2002,* European Parliament History Series, No1, Luxembourg, Publication Office of the European Union.

Reeve, Gillian & Smith, Joan (1986) *Offence of the Realm – How Peace Campaigners get Bugged,* London, CND Publications.

Sharpe, Sybil (2000): *Search And Surveillance : The Movement From Evidence To Information*.: Aldershot ; Burlington, VT. : Ashgate.

Smith, Gavin (2007) Exploring Relations between watchers and watched in control (led) systems: Strategies and tactics, *Surveillance and Society*, 4 (4): 280-313.

Surveillance Studies, online journal: http://library.queensu.ca/ojs/index.php/surveillance-and-society/ accessed 24 August 2015

Surveillance Studies Network http://www.surveillance-studies.net/ Accessed 24 August 2015

Taylor, Phillip M, (2003) *Munitions of the Mind- A history of Propaganda,* Manchester, Manchester University Press.

Thomas, Douglas & Loader, Brian (2000) *Cybercrime. Law Enforcement, Security And Surveillance In The Information Age*, London : Routledge.

Wright, Steve (1987) *New Police Technologies and Sub-State Conflict Control*, Unpublished Thesis submitted for the degree of PhD, Lancaster, University of Lancaster.

Wright, Steve (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/

Zureik, Elia, & Salter, Mark (2005), *Global Surveillance And Policing : Borders, Security, Identity*, Cullompton, Willan.

Steve Wright is a Reader in Applied Global Ethics at Leeds Beckett University. He was the Head of Manchester City Council's controversial Police Monitoring Unit from 1984-1989, which covered alleged police excesses in surveillance and use of force and the so called "Stalker Affair" concerned with the Northern Ireland so-called 'Shoot to Kill' policy. Wright went on to co-found the Omega Foundation in Manchester which does field work on the evolution and deployment of new technologies of political control, including advanced surveillance technologies.