MEDIANZ • VOL 14 NO 2 • 2014
DOI: http://dx.doi.org/10.11157/medianz-vol14iss2id120

- ARTICLE -

Digital Domesday: Saturation Surveillance and the New Serfdom

Graham Murdock

Surveillance and the Erosion of Citizenship

Surveillance can be most usefully thought of 'as any systematic, routine, and focused attention to personal details for a given purpose' (Lyon 2014, 2). As the classified US documents leaked by Edward Snowden from the beginning of 2013 onwards makes clear, over the last decade the surveillance of citizens in Western democracies has become both more intensive and more pervasive. Escalating official concern over the increased threat of terrorist bombings in the wake of the 9/11 attacks on New York and Washington, combined with the exponential growth of readily available Internet data on the location, involvements, tastes, and contacts of individuals, has shifted 'Surveillance practices . . . from targeted scrutiny to mass monitoring' (Lyon 2014, 2).

This movement, from selectivity to saturation, brings into sharp relief the tension that has always been at the heart of democracies, between the government's responsibility to protect citizens' rights and their obligation to guarantee their safety and security. The urge to acquire total knowledge of the civil population is not new. As the compilation of the best-known pre-modern European instance, the *Domesday Book*, demonstrates, it has always been an aspiration of governance.

In 1085, the Norman ruler of England, William, spent Christmas with his closest confidants at Gloucester. Almost two decades had passed since his troops had crossed the Channel and defeated the Saxon king, Harold, at Hastings, investing William with the title of 'Conqueror'. But his realm was not secure. There was the constant threat of invasion and internal insurrection. To consolidate his rule he needed to know who owned what, what taxes he could raise, and where the military capacity he could call on,

---

Graham Murdock is Professor of Culture and Economy at Loughborough University. His research examines the role of communications in the constitution of modernity, the relations between culture, communications, power and inequality through a distinctive critical political economy, and the organisation of public definitions and responses to perceived threats and risks. His writings have been widely anthologised, cited, and incorporated into university curricula around the world and been translated into nineteen languages.

or which could be deployed against him, was located. To find out he commissioned a 'Great Survey' of his occupied country dispatching royal officers to make a detailed inventory of holdings in village and towns across England. It was a monumental task completed with a year and the results recorded in what became to be known as the *Domesday Book* because, like the Last Judgment of God, its findings were final and could not be revised or appealed against. As the *Anglo-Saxon Chronicles* noted at the time, nothing escaped the officers' zealous inspection:

> So very narrowly, indeed, did he commission them to trace it out, that there was not a single hide, nor yard of land, nay moreover (it is shameful to tell, though he thought it no shame to do it), not even an ox, nor a cow, nor a swine was there left, that was not set down in his writ. And all the recorded particulars were afterwards brought to him (Anon n.d.)

Nothing as comprehensively detailed was attempted in England again until the nineteenth century with the first national census of population in 1801, the introduction of a permanent income tax in 1842, and the Return of Owners of Land in 1873. These initiatives however, were launched in a new and very different political and economic context built around three developments. Firstly, ideals of democracy insisted that the state's coercive power be held accountable to parliaments elected by popular vote. Secondly, governments were taking on increased responsibilities for providing basic resources that supported individual self-realization and the overall quality of collective life. Thirdly, the profitability essential to the expansion of capitalism was increasingly coming to rely on personal consumption. Each of these innovations supported a new apparatus of surveillance organised respectively around security, welfare, and marketing.

Building on Patton's useful definition, we can define the contemporary surveillance system as an assemblage of institutional complexes developed for different purposes 'whose unity comes solely from the fact that . . . they "work" together as a functional unity' (Patton 1994, 158). Recovering the histories of these complexes is essential to a full understanding of current developments since the present moment is defined precisely by their progressive incorporation into a single integrated system.

Within this system, control over the digital data that increasingly determines life chances is being ceded to remote centres of power that remain opaque and invisible, concealed behind walls of secrecy erected to protect these centres' conceptions of national security and commercial privilege. The resulting asymmetries in access to the information that informs the actions of the powerful (Lightfoot and Wisniewski 2014) is edging democracies towards a new absolutism. At the same time, the ways in which information on individuals is now being collected, classified and analysed is progressively eroding the rights of citizenship and generating new forms of subjection. We are witnessing the return of serfdom.

Assembling the Surveillance Assemblage:

The Security Complex

William's claim to power was absolute, legitimated by divine right. The population he ruled over was subjected to his unchallengeable authority but entitled to his protection. As his subjects they had no choice but the trade personal liberty against security. This system was challenged and overturned by three revolutions in the space of three decades at the end of the eighteenth century. The French Revolution of 1789 destroyed the French monarchy and declared a republic, and the American Revolution of 1776 and the Haitian Revolution of 1791-1804 (the only successful slave revolt), replaced imperial rule with national self-government. Subjects were transformed into citizens, members of a political community whose governance was determined by free popular elections of the representatives who would make the laws by which they would consent to be governed.

The struggle to extend this core right of citizenship to everyone and create a genuinely inclusive system of representative democracy was protracted and bitter, and remained incomplete in many places at the turn of the twentieth century, including England, where the full female franchise was only finally introduced in 1928. The battle to universalise citizenship was, from the outset, bound up with two pervasive Establishment fears, of popular subversion and insurrection and loss of economic advantage and imperial reach.

The nineteenth century was a period of unprecedented migration, internally, from the countryside to the booming industrial cities, and transnationally, as those dispossessed by hunger and political persecution in their own countries sought refuge and prospects in the rising centres of the new capitalism. In 1849, Karl Marx, having been expelled successively from Prussia, France and Belgium for his radical political views, took up permanent residence in London, where in 1851, he was kept under surveillance by Wilhelm Stieber, an agent using an assumed name and posing as a journalist, dispatched by the Prussian Minster of the Interior. Stieber inveigled his way into the Marx household and compiled a detailed description. Expecting to find po-faced revolutionaries, he is won over by the conviviality and intellectual energy of Marx's circle:

> Marx lives in one of the worst and hence cheapest quarters of London. . . . There is not one piece of good, solid furniture in the entire flat. Everything is broken, tattered and torn, finger-thick dust everywhere, and everything in the greatest disorder. But nothing of this embarrasses Marx or his wife in the least; you are cordially offered a pipe, tobacco, and whatever else there is; a spirited conversation makes up for the domestic defects and in the end you become reconciled because of the company, find it interesting, even original. (quoted in Holmes 2014, 8)

By the end of the century, however, fear of immigrants and their subversive political ideas and activities had escalated and hardened. They had become 'the enemy within', resident in their countries of exile and migration but championing 'alien' ideas. Initial concern focused on anarchist activists who had dramatized their promotion of 'propaganda by the deed' with the series of bomb outrages; assassinating the Russian Tsar Alexander in 1881, and bombing the French Chamber of Deputies in 1893 and the Royal Observatory in London, the following year. The most extensive anarchist campaign occurred in the United States in 1919. In April, over thirty leading political and business figures, including the Attorney General and John D. Rockefeller, were sent packages in the post containing dynamite, and in June bombs were detonated within ninety minutes of each in seven cities across the country, including Philadelphia, home of the Liberty Bell, one of the central symbols of American democracy. The *Philadelphia Inquirer* cemented the popular iconography of threat in a cartoon showing a heavily bearded, swarthy, and Eastern-looking, man holding a torch labelled 'anarchy', creeping under the US flag. The authorities' reaction was rapid with around 10,000 arrested, 3,500 held in detention, and 556 'enemy aliens' eventually deported. The media image of the 'terrorist' forged against this background has proved remarkably resilient with contemporary Jihadists portrayed in almost exactly the same way as the East European anarchists a century earlier.

There are continuities too in the official response, with the two most prominent recent US whistle blowers exposing covert military and intelligence operations, Chelsea (formerly Bradley) Manning and Edward Snowden, being prosecuted under the Espionage Act of 1917, originally introduced during World War I as part of a wider response to the emergence of Germany as a major military and economic power.

In 1909, Britain, perceiving a substantial threat to its industrial and imperial ascendency, had established the Secret Service Bureau, to maintain surveillance over German activities. On the outbreak of war in 1914 the organization was split into two. The Security Service, MI5, (Military Intelligence, Section 5), assumed responsibility for domestic intelligence, alongside the Special Branch of the police force whose first was division was formed in London in 1883 to combat anarchists and militant Irish nationalists. The Secret Intelligence Service (MI6) took charge of foreign intelligence. There was a parallel initiative in the United States with the establishment of the Bureau of Investigation in 1908, the precursor of the Federal Bureau of Investigation (FBI) launched in 1935 and responsible for both criminal investigation and domestic surveillance. The organization of US foreign intelligence however remained dispersed across a number of agencies, including the War Department and the Treasury, until the advent of the Cold War with the Soviet Union and the launch of the Central Intelligence Agency (CIA) in 1947.

The collection of intelligence continued to rely heavily on the labour intensive work of agents, informers, and infiltrators, who kept watch over targeted individuals and went undercover, joining suspect organizations. Like Marx's shadow, Wilhelm Stieber, they

compiled extensive notes of their targets' contacts and conversations, supplemented later by photographs of who they met. Files in the British National Archive, recently made public, reveal that throughout the 1950s, Christopher Hill, a former member of the Communist Party, but by then one of Britain's leading historians and Master of Balliol College, Oxford, was kept under surveillance to establish:

> the identity of his contacts at the University and in the cultural field more generally, and to obtain the names of intellectuals sympathetic to the party who may not already be known to us (Norton-Taylor 2014, 13)

Meetings were recorded in detail by an informant, code-named, Ratcatcher. While systematic and extensive, the surveillance of British Communists, fellow travellers, and their friends, remained bounded. On the other side of the Cold War divide however, monitoring of potential 'enemies within' was taking place on an industrial scale. It is estimated that The Ministry for State Security (Stasi) in East Germany employed up to two million permanent and occasional informers (Koehler 2000, 8-9) with the results of their labours stored in paper files occupying miles of shelving.

As the Stasi files also reveal however, the intensive collection of 'human intelligence' (HUMINT) was supplemented by extensive 'signals intelligence' (SIGINT) based on the interception of telegraphic traffic and telephone calls.

Steaming open letters had long been part of the standard armoury of surveillance. MI5 were at one point reading up to ten letters a day sent to and from Christopher Hill and another leading left wing historian, Eric Hobsbawm, who remained a life-long member of the Communist Party (Norton-Taylor 2014, 1). But the invention of the telegraph and later the telephone offered access to extensive new sources of intelligence. Perfecting ways of tapping into these communication flows and breaking the codes if messages were encrypted, moved rapidly up the list of priorities for effective surveillance. Efforts originated in attempts to intercept military signals during World War I, hence the description, 'signals intelligence', but they continued into peacetime, spurred on by the Bolshevik seizure of power in Russia, after a civil war to which both Britain and the United States had committed troops to support anti Bolshevik forces. In May 1919, the US Government founded the Cypher Bureau (also known as the Black Chamber) to develop interception and decoding techniques. In 1952, with advent of the Cold War this became the National Security Agency (NSA).

1919 also saw the amalgamation of the British army and navy signals intelligence units that had operated during World War I to form the Government Code and Cypher School (GC&CS). Peace time operations focused mainly on intercepting diplomatic cables, particularly from the Soviet Union. With the advent of the Second World War they returned to tracking military communications successfully breaking the codes used by the Enigma and Lorenz cipher machines employed to encrypt telegraphic messages passing between the German High Command and operational commands across

occupied Europe. A key part of this effort was the calculating capacity provided by Colossus, the world's first programmable computer. With the War's end in 1946, GC&CS was renamed The Government Communications Headquarters (GCHQ) and later moved to a larger site with enhanced facilities to intercept and record telephone and radio traffic. That same year, a secret arrangement between the United Kingdom and United States governments established cooperation in the collection and sharing of signals intelligence. This alliance was later extended to three other major allied countries, Canada, Australia and New Zealand, to form the 'Five Eyes' network.

The Welfare Complex

Protecting national borders from external attack and maintaining order within them had long been seen as the bedrock obligation of states. But as philosophies of citizenship gained ground, governments in Western democracies increasingly assumed additional responsibilities for guaranteeing minimum standards of welfare. The worst excesses of capitalist exploitation were curbed and regulated, and over time an extended array of publicly provided material and cultural facilities and resources were introduced, funded out of revenues raised by systems of taxation that were progressively extended from a minority of high income earners to a universal payment. By the early 1950s these subsidised resources typically included state pensions, unemployment benefits, subsidised housing, free schooling, public libraries, and health care free at the point of use. Each of these complexes generated a substantial paper trail tracking users' locations, activities, conditions, and preferences. But they remained separate, dispersed across a range of institutional sites.

The Marketing Complex

The extension of citizenship, as both an ideal and an array of institutions intended to support full and equal participation in social and political life, was accompanied by the rise of the 'consumer' and the seductive promise, central to capital's continued expansion, that markets were the preeminent space of personal freedom and self-realisation, and that commodities offered the most eloquent language through which to speak to others about ones achievements, tastes, aspirations. The years between and after the two world wars saw the rhetorical appeal of consumption supported by a series of innovations in research designed to map markets and direct purchasing. In 1925, Neil McElroy joined the largest manufacturer of household products, Proctor and Gamble, and began developing techniques of brand differentiation that cemented associations between brands and life styles. In 1929 Edward Bernays, the nephew of Sigmund Freud, launched a campaign to persuade more women to smoke by paying young women to march in the New York Easter Parade and on a given signal to light up cigarettes while holding aloft placards with the slogan, 'Torches of Freedom'. In the following decade, Arthur Neilsen began analysing the potential of the radio market as a site for product promotion and devising a ratings system for programming that became the key mechanism for determining the prices advertisers paid for broadcast slots. By

the 1960s, recovery from wartime austerity and steadily rising real wages across the advanced capitalist economies had generated a very extensive marketing complex based on research intelligence that defined increasingly segmented markets (with the 'invention' of the 'teenager' and later the 'tween') and propelled the promotion of life styles through advertising that anchored product appeals in clusters of carefully orchestrated connotations.

There were biographical intersections between key figures involved in developing the marketing and security complexes. Edward Bernays had begun his career in the US Government's propaganda arm in World War I, the Committee on Public Information, and was invited by President Woodrow Wilson to attend the Paris Peace Conference in 1919. He saw his peacetime promotional activities as a direct continuation of his wartime mission but because of the negative associations surrounding the term 'propaganda' opted to describe them as 'public relations', a phrase he popularized in his 1923 book, *Crystallizing Public Opinion.* In 1957, Neil McElroy resigned his position as president of Proctor and Gamble to become Secretary of Defense in the Eisenhower Administration with responsibility for directing an array of operations in both human and signals intelligence. Despite these personal ties, and extensive common borrowings from a shared research literature on persuasion and popular mobilization, security and marketing remained largely separate domains.

Reconstructing Surveillance: Saturation and Integration

The integration of public relations and intelligence has been propelled by the intersection of the three interventions: the fundamental technological shift from analogue to digital modes of communication and the attempts to address both economic and political crises. Corporations and governments have come to see digital technologies as powerful new tools in their struggles to restore profitability and combat 'new' forms of terrorism and social protest. Both ambitions involve saturation surveillance.

Digital Dividends and Big Data

Analogue communication systems parceled information out into separate forms—paper files, photographs, sound recordings, film and video—each based on a discrete technology with only limited possibilities for consolidation. By translating all forms of communication—text, voice, sound, still and moving images—into the universal language of computing and expressing them as arrays of 'zeroes' and 'ones', digital coding allowed information from any source to be combined and integrated into a single data set. Developments in the supply, storage, and analysis of digital communications have converged to convert this promise into practical routines, providing a powerful new technological basis for saturation surveillance.

The last two decades have seen the internet emerge as a mass utility. Access has become increasingly ubiquitous and mobile, migrating from desk top machines to laptops, to smart phones and tablets with ever increasing memory capacity, processing power, and applications. Fixed line dial-up links have been replaced by interlocking wifi zones, providing always-on, always-there, continuous connectivity. This new online space has been increasingly filled with social media sites, which encourage users to share an ever-expanding range of personal data. This activity produces a massively enlarged pool of information on individual users. In addition to the direct content of emails and web postings, every touch of the keyboard or screen generates valuable metadata, 'data about data', identifying 'the location from which the message was sent, when it was sent . . . the recipient(s)' web address', and more (Sullivan 2013, 90). Even if the content of messages is not interrogated, analysing this meta-material 'can now provide a detailed portrait of who people know, where they go, and their daily routines' (*The Economist* 2013, para 8). As the Snowden disclosures reveal, 'while specific cases of monitoring the content of phone calls and examining text messages exist as well', the extremely large-scale collecting and analysis of metadata has become 'central to the NSA's surveillance program' (Lyon 2014, 3). The ability to detect patterns in this sea of data, to 'connect up the dots', in a favoured security community phrase, depends on having sufficient computer storage and processing power.

Over the last two decades the costs of storing a gigabyte of digital data have dropped dramatically, from almost two thousand dollars in 1993 to four cents by 2013 (Copeland 2013). Over the same period computer processing power has increased exponentially. In 1996, the year after the launch of Google and Yahoo, the world's most powerful computer, built by Hitachi in Japan, was achieving processing speeds of 368.2 gigaflops (billions of operations a second). By 2014 the leading machine, the Tianhe-2, developed by China's National University of Defense Technology was running at 33.86 petraflops (quadrillions of calculations a second). Six of the other top ten machines were located in the United States including one assigned to an undisclosed US government site (Top 50 Supercomputer Sites 2014).

These innovations in computing and network capacity have generated massive pools of information, dubbed Big Data (see Mayer-Schonberger and Cukier 2013). This new reservoir of intelligence is distinguished from past repositories by its huge volume, its compilation in almost real time, its comprehensiveness, its ability to be linked to other data sets, and its support for detailed analysis of individuals (Kitchin 2014, 262). Activating this potential however requires human judgments to be automated, employing computer software programs, algorithms, to conduct analysis. The discretion previously exercised by individual analysts is replaced by machine generated searches for links and patterns governed by whatever assumptions were built into the program. This shift has three major consequences. Firstly, persons under surveillance are translated from bodily individuals acting in concrete spaces to 'data doubles' defined by the traces they leave as they interact with digital devices. Secondly, by focusing on correlation, on linkages, rather than causation, it focuses attention on 'what is

happening now and what might happen next? Rather than asking "Why?"', placing more weight 'on managing consequences rather than research on the underlying causes of . . . disorder' (Lyon 2014, 6). Thirdly, the detection of a pattern is sufficient in itself to classify an individual as 'suspicious', reversing the burden of proof on which the rule of law in democracies rests. People are classified as potentially guilty 'by association', and judged 'not on what they did, but on what we predict they might do' (Mayer-Schonberger and Cukier 2013, 176).

Technological innovations in hardware and software have combined to deliver a substantial digital dividend to the drive for saturation surveillance, but to explain why this degree of comprehensiveness has come to be seen as essential we need to place it firmly in the context of responses to interlocking economic and political crises.

Regenerating Profitability: Surveillance as a Business Model.

In the mid-1970s mature capitalist economies experienced a severe crisis of profitability. Coinciding with a deepening disillusion with state management this opened the way for policies driven by a resurgence of a neo-liberal ideology aggressively promoting the extension of market dynamics as the only 'realistic' solution. Led by the Thatcher governments in the UK and the Reagan administration in the US, public assets were sold off, the regulation of business relaxed, company taxes reduced, and the rights of organised labour whittled away. Corporations were allowed to move into areas they were previously locked out of and granted greater freedom of action.

As part of the wider drive to privatise public holdings or 'monetize' their value more fully, there has been a concerted push to open access to public sector data bases to commercial companies. The result has been an increasing integration of the welfare and marketing complexes. Health records have been a particular site of contention. In November 2014, it was revealed that, despite repeated assurances to the contrary, between 1989 and 2010 records of patients passing through the public hospitals of the British National Health Service, containing their dates of birth, post codes, and medical histories, had been sold to insurers wanting to adjust their premiums (BBC 2014). This was not the only instance of information on individuals collected by the welfare complex being transferred to private interests. The partial sale of the Royal Mail postal service to commercial investors in 2013 had included the Postcode Address File (PAF) information that when combined with other readily available data offered a new resource for targeted marketing and a strong source of revenue for the Mail's new owners (Sparrow 2014, 12). And at the time of writing, proposals to sell personal financial data collected for tax purposes are under active discussion in Britain (Mason 2014)

This reorganization of production and provision was accompanied by a concerted push to expand and accelerate consumption. Companies looked for ways of salami slicing markets into ever smaller niches, thickening the symbolic weight attached to brands,

defining and targeting potential consumers more precisely, and encouraging them to convert their desires into purchases by borrowing on one or more of the rapidly expanding array of credit and store cards. Marketing companies harvested the individual data generated by card purchases, combining it with publicly available information from census returns and other government data bases, to identify and track consumers more precisely and develop fuller profiles of their views and tastes (Gandy 1993).

The arrival of the Internet, and its emergence as a mass utility, rapidly expanded the options available to corporations wanting to intensify consumption. The companies that came to dominate key areas of everyday internet use, Amazon (1994) and eBay (1995) in on- line retailing; Google and Yahoo (1995) in search and email; and Facebook (2004) in social networking, adopted commercial surveillance as their preferred business model. Every time users logged on, typed on their keyboard, touched their screen, or activated their mobile phone, they supplied valuable information about themselves, their tastes and activities, where they were located, who they were connected to and what they talked about, that the platform owner could use to target them more effectively themselves and sell on to advertisers wanting to address potential purchasers with personalised appeals. Because the Net was subject to far less regulation than the established print and audio-visual media, companies wishing to use it for product promotion were able to take full advantage of its immersive and interactive qualities to develop forms of advertising that were more thoroughly integrated into the flow of on-line activity through product placement, sponsored blogs and which offered the pleasures of playful engagement. At the same time, the expansion of frictionless on-line payment systems, led by Pay Pal (bought by eBay in 2002), encouraged increased immediate and impulse buying.

The early utopian dreams surrounding the Internet promoted its interactive capacity as a fatal blow to the top-down structures of power that governed the established media. Vertical hierarchies would give way to horizontal networks, and the centralised distribution of pre-packaged material would be displaced by dispersed collaborative creativity. The Web would transform consumers into co-producers who actively contributed to the material they logged onto and downloaded. This vision of openness however, rapidly bumped up against the corporate consolidation of control over the central territory of the Net and the key players' concerted appropriation of users' labour. In return for 'free' access to computer capacity, participants in social media sites, led by Facebook, were required to cede the intellectual property rights to everything they posted. The user-friendly rhetoric of 'prosumption' concealed the reality of a new serfdom, which consigned users to toil in virtual fields owned by the new digital landlords and relinquish all title to the fruits of their labours (Comor 2010; Fuchs 2013).

As the classified files leaked by Edward Snowden make clear, the National Security Agency was siphoning off huge amounts of this user generated data as it moved across the open internet, interrogating email content, tracking the location of cell phones,

'piggybacking' on the tools used by advertisers to target consumers, and undermining the encryption systems devised by commercial internet sites to protect their users' privacy. This material was added to the intelligence being gathered by the security agencies to form an unprecedented pool of information. The central initiative in this concerted effort to tap into everyday internet use was codenamed PRISM, the Planning Tool for Resource Integration, Synchronisation and Management, a designation that simultaneously announced and celebrated the convergence of the security and marketing complexes. It is part of an array of programs whose employment crosses national borders.

Global Security: Global Reach

As mentioned earlier, the National Security Agency is the hub of a global surveillance network known as the 'Five Eyes', made up of its major allies, including Great Britain and New Zealand. The extent to which intelligence is shared among participants has been a focus of contention with Edward Snowden's revelations being met with official denials.

NSA's Xkeyscore program allows analysts to search both metadata and the content of individuals' emails, browsing histories, and interactions, by completing an on-line form providing broad justifications for a search. Edward Snowden claimed that in the course of his contract work for the Agency, he 'routinely came across the communications of New Zealanders' and that New Zealand's principle security agency, The Government Communications Security Bureau (GCSB) had access to Xkeyscore (Kampmark 2014, 2). This claim was roundly rejected by the New Zealand Prime Minister, John Key, who insisted that 'GCSB does not collect mass metadata on New Zealanders, but he declined to comment on Xkeyscore adding that 'we don't discuss the specific programs the GCSB may, or may not use' (Key 2014, 1). Open questions also surround New Zealand's involvement in another major element in the global security system.

The Southern Cross undersea cable network linking Australia and New Zealand to the West Coast of the United States is of key strategic importance for the United States' security interests in the Southern Hemisphere. In an effort to increase intelligence capacity a project codenamed 'Speargun', to tap into the cable and collect metadata on the traffic passing through it, was floated. The initial phase, of installing the system, was scheduled to be completed by late 2012–early 2013, to be followed in mid-2013 by active probes of metadata. The New Zealand government denied that this project 'ever got off the ground' but NASA documents record the intercept capacity as having been installed and awaiting a change in New Zealand law permitting the government to collect intelligence on its own citizens as well as foreign nationals, to become operational (Greenwald and Gallagher 2014).

The Bill expanding the powers of the Government Communications Security Bureau was passed in August 2013 by sixty one votes to fifty nine after a heated debate. It was

introduced after John Key was obliged to issue an official apology to the Internet entrepreneur, Kim Schmitz, who had changed his name to Kim Dotcom in 2005, and become a 'permanent resident' of New Zealand under the terms of the 2009 Immigration Act, when it was established that the GCSB had unlawfully intercepted his communications in violation of the legal prohibition on surveillance of New Zealanders. As the report compiled by the Inspector General of intelligence and Security, Paul Neazor, reaffirmed, because GCSB's remit was restricted to collecting intelligence 'about the capabilities, intentions, or activities of a foreign organization or foreign person . . . if the person is a citizen of New Zealand or a permanent resident his or her communications are protected' (Scoop 2012, 3) The revision to the legal framework removed this protection and translated the GCSB from an agency confined to collecting and analysing foreign intelligence to a domestic surveillance agency. Despite the Prime Minister's assurances that surveillance will remain targeted and only undertaken at the specific request of a domestic law enforcement or security agency, experience elsewhere suggests a strong impetus to exceed these boundaries.

In Britain, under current legislation, interceptions of communications traffic require authorisation from the Interception of Communications Commissioner who is charged with ensuring that requests are appropriate and proportionate. Reporting in April 2014, on his activities during 2013, the present Commissioner, Sir Anthony May, was moved to remark that the 514,608 requests submitted to his office over the year, ninety nine percent of which came from law enforcement and intelligence agencies, 'seems to me to be a very large number. It has the feeling of being too many' (May 2014, 26). In summarising his findings however, he put aside his qualms and concluded that 'the interception agencies do not engage in indiscriminate mass intrusion' (May 2014, 56). Two months later, the major mobile phone operator, Vodafone, revealed the existence of secret wires attached to its networks allowing government agencies direct access to all conversations passing through them (Garside 2014). Just over a week later, the government's top security official argued that since the sites involved were located outside the UK, individuals' uses of Google, Facebook, Twitter and YouTube were classified as 'external communications' and therefore fell outside the scope of current legislation (Dodd 2014a). This admission is at odds with an earlier government denial that British analysts based at GCHQ were 'accessing communications content via the PRISM programme'. General access would be in clear contravention of the formal requirement that any request for intercept information from the US be signed by a Minister, and would, as the Intelligence and Security Committee of Parliament pointed out, 'constitute a serious violation of the rights of UK citizens' (Intelligence and Security Committee of Parliament 2013:1). Leaked NASA documents however, confirmed that 'special programmes for GCHQ exist for focussed Prism processing' of material of particular interest to British intelligence and that in the year to May 2102, GCHQ generated 197 intelligence reports based on Prism data, a 137% increase on the year before. How many of these reports had Ministerial authorisation is not known since as a

GCHQ spokesman reiterated, 'we do not comment on intelligence matters' (Hopkins, 2013).

But why do the intelligence agencies in Western democracies feel the need to assemble the largest possible collection of Big Data? To answer this question we need to examine shifts in the political environment and changing official perceptions of threats to order and security.

From 'Old' to 'New' Terrorism

As noted earlier, alongside concern about the hostile intentions of foreign powers, led by Germany, the construction of the modern security complex on both sides of the Atlantic was in large part a response to bombings committed by anarchist groups, and in Britain by Irish nationalists. These early instances of direct violent action cemented an enduring conception of 'terrorist' activity as a para-military incursion, involving organised cells carrying out the orders of a high command. This image offered a plausible characterisation of a number of the most prominent initiatives of the post war years, from the Irish Republican Army (IRA) bombing campaign in mainland Britain and the Red Army Faction (RAF) in Germany, to the Basque separatist ETA movement in Spain. In 1994 however the IRA declared a complete cessation of military operations followed in 1998 by the RAF announcing that they were ending their urban guerrilla campaign.

In 1993 however, Islamic extremists led by Ramzi Yousef detonated a truck bomb below the North Tower (Tower One) of the World Trade Centre in New York, intending to demolish both towers by crashing the first tower into the second one. They did not succeed but killed six people and injured over a thousand in the attempt. Eight years later, on September 11th 2001, both towers were destroyed when another group of Islamist activists crashed passenger airliners into them. There was a connection between the two attempts. Yousef uncle, Khaled Sheik Mohammed, who had supported his nephew's operation financially was later alleged to have been the head of al-Qaeda's propaganda operations and named as the main architect of the 9/11 attacks in the official commission report on the events. He was eventually arrested in Pakistan 2003, where he was in hiding, and taken into US custody. The security agencies inability to prevent either of the attacks however pointed to a substantial intelligence failure.

In response, commentators argued that identifying potential terrorists had become more difficult because the familiar 'old', paramilitary, styles of organization were being replaced by 'new', more fluid and fuzzy forms (see Neumann 2009). They saw vertical chains of command giving way to dispersed networks, with activities planned by small groups or individuals who had been inspired by ideological appeals but were not formal members of an organisation. In place of campaigns for national self-determination or opposition to a particular state formation, they saw emerging forms of terrorism as part of a transnational movement of radicalised adherents to a fundamentalist interpretation

of Islam, motivated variously by retaliation for the US led invasions and occupations of Iraq and Afghanistan, demands for the restitution of respect for Islamic culture, the introduction of Sharia Law, and the restoration of the Caliphate.

On the 7th July 2005, four young men detonated rucksack bombs in London, three in the underground system and one on the upper deck of a bus, killing themselves and fifty two other people and injuring more than seven hundred. In a video recording the group's leader, Mohammed Sidique Khan, explained that their action was a response to Britain's support for military action in Muslim countries. All four were part of the diaspora from Britain's former colonial territories. Three were the British born sons of migrants from Pakistan and the fourth was born in Jamaica. At first glance there was nothing exceptional about them. Khan was married with a child and employed as a learning mentor in a primary school. One of others lived with his parents and worked in a fish and chip shop. It was precisely this appearance of ordinariness that caused most concern. As the then Prime Minister, Tony Blair, declared at the time, 'the rules of the game are changing' (quoted in Armstrong 2012, 7). Enemies within were no longer arriving from overseas, they were British nationals and gave every appearance of being assimilated into British society. Concern intensified in 2013 when an off-duty soldier, Lee Rigby, was attacked and killed on his way back to his barracks in south London by two British born converts to radicalised Islam. Launching a week designed to raise public awareness in November 2014, the head of police counter-terrorism operations, Mark Rowley, forcefully restated the argument that changed conditions required saturation surveillance, including of Internet traffic.

> The danger posed by violent extremists has evolved. They are no longer a problem solely stemming from countries far away. Now, they are home-grown, in our communities, radicalised by images and messages they read on social media and prepared to kill for their cause (quoted in Dodd 2014b, 1).

A week later the Intelligence and Security Committee of Parliament published a detailed report on the murder of Lee Rigby, revealing that one assailant had been 'a high priority for MI5' who had 'put significant effort into investigating him and employed a broad range of intrusive techniques' none of which had 'revealed any evidence of attack planning'. In contrast, the second assailant had been classified as a low level risk for whom 'intrusive action would not have been justified' (Intelligence and Security Committee 2014, 1). However, the Committee noted that the security services had not had access to an online exchange in which he had talked about murdering a British soldier in the most graphic terms, arguing that had they seen it 'there is a significant possibility that [they] would have been able to prevent the attack' (Intelligence and Security Committee 2014, 2). Rather than concluding that there had been major failures in MI5's intelligence operations the Committee transferred blame to the web site, later revealed as Facebook, for not regarding 'themselves as under any obligation to ensure that they identify such threats, or report them to the authorities' and therefore, unwittingly, 'providing a safe haven for terrorists' (Intelligence and Security Committee

2014, 2). Their conclusion was unambiguous, 'the capability of Agencies to access the communications of their targets is essential to their ability to detect and prevent terrorist threats in the UK' with the clear implication that if web sites would not furnish this information voluntarily they must be compelled to do so (Intelligence and Security Committee 2014, 2).

Recent research sponsored by the National Research Council of the National Academies in the United States however, suggests that amassing ever larger pools of Big Data may be self-defeating because the ever increasingly volume and heterogeneity of the digital information being collected is outstripping the computer processing power and algorithmic tools available to tackle it (Committee on the Analysis of Massive data 2013, 26). As, Coleen Rowley, a former FBI agent tartly noted: 'if you're looking for a needle in a haystack, how does it help to add hay?' (Rowley 2014, 42).

The urge to build an ever larger haystack out of harvested digital data has been reinforced by the impetus to stretch the definition of 'terrorism' and enlarge the conception of threat.

New Enemies Within

Radicalised Islamic militants were not the only group subjected to the new 'rules of the game' drawn up in the wake of the 9/11 attacks. In the United States, as Coleen Rowley has argued, while the sixteen names on the CIA's terrorist prior to the attacks were probably 'were justified, . . . there's no way the million names reportedly now on the 'terrorist identities datamart environment' list can be very accurate' (Rowley 2014, 42).

The British government's response to 9/11 was to declare a state of 'public emergency threatening the life of the nation'. This condition, originally intended as a temporary measure, was never rescinded leading the Parliamentary Joint Committee on Human Rights to complain in 2010 that by 'normalising the exceptional' the government was claiming 'that exceptional measures require less justification than when times are normal' and that 'courts and other accountability mechanisms should defer to the Government's assessment of what measures are required' (House of Lords/House of Commons 2010: Section 2, para 16). The measures seen to be 'required' included stretching the definition of the 'enemies within' to include actions that disrupted corporate activity. This generalised a definition that had received strong official endorsement in the mid 1980s.

In 1984, miners across Britain staged a national strike to protest the threat of wholesale pit closures. The action lasted for a year and was one of bitterest disputes in the country's industrial history. Taking their cue from the then Prime Minister, Margaret Thatcher, who had no hesitation in denouncing the miners as 'the enemy within', MI5 deployed the full range of 'dirty tricks' to discredit the strikers and their leadership, in a 'mobilization of [the] covert state' which the most authoritative account of the strike has described as 'unparalleled in modern peace-time Britain' (Milne 2014, 390).

This enlarged definition of 'enemies within' was invested with statutory authority in 1994 when the Intelligence Service Act formally defined the responsibilities of GCHQ as working 'in the interests of national security, with particular reference to the defence and foreign polices of Her Majesty's government' together with advancing the 'economic well-being of the United Kingdom'. By expanding the definition of the 'enemy' to include groups that disrupt economic activity and corporate expansion, this very general brief gave added impetus to the shift from selective to saturation surveillance.

As well as extended monitoring, actions by environmental and animal rights groups directed at leading energy, agri-business and pharmaceutical companies, have been increasing subject to special provisions, such as stop and search, introduced under the Terrorism Acts of 2000 and 2006. As the listing of 'other forms of terrorism' alongside 'al-Qaeda inspired' and 'Northern Ireland related' actions, in the report of the Independent Reviewer of the operation of the Acts confirms, measures originally intended to be selective have become pervasive (Armstrong 2012, 18) with the report's author noting 'the extreme breadth of the definition of 'terrorism' in the UK' (Armstrong 2012, 18).

The monitoring of 'domestic extremism' has also been extended to journalists reporting on state and corporate misconduct. Six members of the National Union of Journalists (NUJ) in Britain are currently bringing a case against the Metropolitan Police Commissioner and the Home Secretary challenging their continuing surveillance by the National Domestic Extremism and Disorder Intelligence Unit. As the NUJ's general secretary, Michelle Stanistreet, noted 'there is no justification for treating journalists as criminals or enemies of the state' for fulfilling their responsibility to expose abuses of power on behalf of the citizenry (quoted in National Union of Journalists 2014, 1). Nor was there any clear justification for the police to conduct detailed analysis of the phone records of 1,757 staff working for the *Times, Sunday Times* and *Sun* newspapers after the material had been sent to them in error by the telephone operator, Vodafone Greenslade 2014, 32) It is one further sign of the drift towards absolutism.

The New Absolutism

The revolutionary crowds that filled the streets of Paris in 1789 demanded full citizenship grounded in liberty, equality, and mutuality. The move from selective to saturation surveillance undermines these core principles and returns us to a condition of serfdom, in which, like William the Conqueror's subjects, we look to increasingly unaccountable governmental and commercial powers to guarantee our safety and security and direct our social participation. The result is a profound contradiction at the heart of formally democratic societies. 'As the details of our daily lives become more transparent to the organisations surveilling us, their own activities become less and less easy to discern' (Lyon 2013, 12).

William the Conqueror's officers meticulously counted every yard of land and every ox, cow, and pig in his kingdom. The contemporary apparatus of surveillance records every email, every posting, every screen page viewed, every person contacted or included in a circle of 'friends'. We have reinvented the Domesday Book for digital times.

The key issues raised by saturation surveillance concern not simply the wholesale suspension of personal privacy involved in collecting information on individuals indiscriminately, but its subsequent deployment to compile group 'profiles' on the basis of their members having something in common. As David Lyon has argued, '*social sorting* is primarily what today's surveillance achieves' (Lyon 2013, 13). This process has pervasive consequences for the allocation of rewards, life chances, and punishments, from the likelihood of being stopped and searched more frequently on the street, to the chances of obtaining credit, or being refused employment. Nor is this 'sorting' random. It is mapped onto and reinforces prevailing structures of inequality and 'contributes to the cumulative disadvantage that weighs down, isolates, excludes, and ultimately widens the gaps between those at the top, and nearly everyone else' (Gandy 2011, 176). In a self-fulfilling process, the ruling categories of 'dangerousness' and 'undesirability' that underpin the algorithms that sort Big Data are recycled in popular media as stereotypes, reinforcing the everyday suspicions and discriminations that confirm the subordination of negatively categorised groups. Our new digital Domesday Books not only compromise liberty and equality, they corrode solidarity and a sense of shared fate.

The anonymous writers of the *Anglo-Saxon Chronicles* commented critically on William the Conqueror's obsessive drive to record every possible holding on his lands, noting that 'it is shameful to tell, though he thought no shame to do it'. This stricture, on the mania for completeness, applies with renewed force to the saturation digital surveillance systems put in place by the governments of the United States, the United Kingdom, and their principal allies. In societies claiming to be democracies, for the state to behave like a feudal monarchy and to think 'no shame to do it' is a fundamental betrayal of the citizens' rights on which the system rests.

References

Anon. n.d. *The Anglo-Saxon Chronicles,* AD 1085. Accessed November 20th 2014. http://www.gutenberg.org/files/657/657.txt

Armstrong, David. 2012. *The Terrorism Acts in 2011: Report of the Independent Reviewer on the Operation of the Terrorism Act of 2000 and Part 1 of the Terrorism Act 2006.* London. The Stationery Office.

BBC. 2014. 'Medical Records Rules Broken, NHS Admits'. Accessed 24th November 2014. www.bbc.co.uk/news/health-2632974

Committee on the Analysis of Massive Data –National Research council of the National Academies. 2013. *Frontiers in Massive Data Analysis.* Washington DC. The National Academic Press.

Comor, Ed. 2010. 'Contextualising and Critiquing the Fantastic Prosumer: Power, Alienation and Hegemony'. *Critical Sociology* 37 (3): 309-27.

Copeland, M.V. 2013. '*WIRED* 20th Anniversary: Storage'. *Wired Magazine,* 16 April. Accessed 20 November 2014. http://www.wired.com/magazine/wired-20th-anniversary/

Dodd, Vikram. 2014a. 'State internet snoopers exploit legal loopholes'. *The Guardian,* June 19.

Dodd, Vikram. 2014b. 'Rigby inquiry failed to seek our witnesses'. *The Guardian,* November 24.

Fuchs, Christian. 2013. *Digital Labour and Karl Marx.* London. Routledge.

Gandy, Oscar Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, CO: Westview Press.

Garside, Juliette. 2014. 'Vodafone reveals mass surveillance'. *The Guardian,* 6 June. Accessed 2 December 2014. http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

Greenslade, Roy. 2014. 'Police at war with press as the access phone records'. *The Guardian,* 1 December. 32.

Greenwald, Glenn and Ryan Gallagher. 2014. 'New Zealand Launched Mass Surveillance Project While Publicly Denying It'. 15 September. Accessed 17 January 2015. https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/

Holmes, Rachel. 2014. *Eleanor Marx: A Life.* London. Bloomsbury

Hopkins, Nick. 2013. 'US Gathering Secret Intelligence via Covert NSA Operations'. *The Guardian,* 7 June . Accessed 2 December 2014. http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

House of Commons/House of Lords. 2010. *Joint Committee on Human Rights- Counter-Terrorism Policy and Human Rights. Seventeenth Report: Bring Human Rights Back In.* London. The Stationary Office. HL Paper 86.

Intelligence and Security Committee of Parliament. 2013. 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme'. News Archive 17th July. Accessed 20 November 2014. http://isc.independent.gov.uk.

Intelligence and Security Committee of Parliament. 2014. 'Press Release'. News Archive November 25. Accessed 25 November 2014. http://isc.independent.gov.uk.

Kampmark, Binoy. 2014. 'Mass surveillance in New Zealand', *Counterpunch*. 16 September. Accessed 26 November 2014. http://www.counterpunch.org/2014/09/16/mass-surveillance-in-new-zealand/

Key, John. 2014. 'PM responds to incorrect surveillance claims.' Accessed 20 November 2014. http://beehive.govt.nz/release/pm-responds-incorrect-surveillance-claims

Kitchin, R. 2014. 'Big Data and human geography: Opportunities, challenges and risks', *Dialogues in Human Geography* 3 (3): 262-67.

Koehler, John O. 2000. *Stasi: The Untold Story of East Germany's Secret Police.* New York: Basic Books [New Edition].

Lightfoot, Geoffrey and Tomasz Piotr Wisniewski. 2014. 'Information asymmetry and power in surveillance societies'. Abstract. http://ssrn/abstract=2383166

Lyon, David. 2013. 'Introduction'. In *Liquid Surveillance: A Conversation,* edited by Zygmunt Bauman, and David Lyon, 1-17. Cambridge: Polity Press.

Lyon, David. 2014. 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique.' *Big Data & Society* 1 (1): 1-13.

May, Sir Anthony. 2014. *2013 Annual Report of the Interception of Communications Commissioner.* London. House of Commons HC1184.

Mason, Rowena. 2014. 'HMCR to sell taxpayers' data'. *The Guardian,* April 19.

Mayer-Schonberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think.* London: John Murray.

Milne, Seumas. 2014. *The Enemy Within: The Secret War Against the Miners.* 3rd ed. London: Verso.

National Union of Journalists. 2014. 'NUJ members under police surveillance mount collective legal challenge'. *News,* 20 November. www.nuj.org.uk/home

Neumann, Peter O. 2009. *Old and New Terrorism.* Cambridge: Polity Press.

Norton-Taylor, Richard. 2014. 'MI5 tapped private lives of left wing historians'. *The Guardian,* 24 October.

Patton. P. 1994. 'MetamorphoLogic: Bodies and Powers in *A Thousand Plateaus'. Journal of The British Society for Phenomenology* 25 (2): 157-69.

Rowley, Coleen. 2014. 'The Bigger the Haystack, the Harder the Terrorist is to Find'. *The Guardian,* 29 November. Accessed 2 December 2014. http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks

Scoop. 2012. 'Text: Neazor Report on GCSB and Kim Dotcom'. *Scoop: Independent News,* 27 September. Accessed 26th November 2014. http://www.scoop.co.nz/stories/print.html?path=HL1209/S00161/text-neazor

Sparrow, Andrew. 2014. 'Ministers Criticised for Selling Postcode Data'. *The Guardian,* March 17.

Sullivan, John L. 2013. 'Uncovering The Data Panopticon: The Urgent Need for Critical Scholarship in an Era of Corporate and Government Surveillance'. *The Political Economy*

of Communication 1 (2): 89-94. Accessed December 2, 2014. http://www.polecom.org/index.php/polecom/article/view/23/192

The Economist. 2013. 'Surveillance: Look Who's Listening'. 15 June. Accessed 20 November . http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

Top 500 Supercomputer Sites. 2014. Accessed 2 November. www.top500.org