# State of surveillance:

## the NSA Files and the global fightback

Ben Hayes

*[E]ven if you're not doing anything wrong you're being watched and recorded. And the storage capability of these systems increases every year consistently by orders of magnitude to where it's getting to the point where you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody even by a wrong call. And then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with. And attack you on that basis to sort to derive suspicion from an innocent life and paint anyone in the context of a wrongdoer...*
- Edward Snowden, June 2013.

### The surveillance state laid bare

If anyone told us anything about the state of power in 2013 it was Edward Snowden, who revealed that the surveillance capabilities of some of the democratic governments of the West are such that they can access almost anything their citizens do online or over a fixed or mobile telephone in the absence of meaningful democratic or judicial controls.

These powers are most advanced in the USA-UK led "Five Eyes" alliance (which also includes Australia, Canada and New Zealand) but many other European countries and NATO partners are known or believed to have advanced surveillance capabilities and to have cooperated closely with the NSA (the National Security Agency of the USA) and GCHQ (the UK Government Communications Headquarters). With a booming global surveillance industry on hand to help them, it is simply inconceivable that many less democratic governments are not engaged in the same practices.

It's hardly news that spies spy, or that the powerful use surveillance and subversion to maintain their power and competitive advantage. In this sense the USA-UK hacking of top politicians' phone calls is something of a convenient sideshow (the real story is the ease with which they did it); what's new and important for the state of power is the simplicity with which individuals and entire populations can be placed under surveillance, the pivotal role that private companies play in facilitating this surveillance, and the lack of power and autonomy that we as individuals have to decide how we are governed and what happens to information about us.

In response to the revelations, newspaper editors and government whistle-blowers have joined more than 300 NGOs and 500 prominent authors from across the world in demanding an end to mass, indiscriminate surveillance; as I write a statement by "Academics Against Mass Surveillance" is also doing the rounds. Longstanding national campaigns against surveillance have been rejuvenated by the Snowden revelations and a host of parliaments and inter-governmental organisations are problematising the issue for the first time. But by no means are these still-growing campaigns a guarantee of meaningful reform. This paper looks at some of the key debates around surveillance reform and the battles ahead.

### Key revelations

Only a tiny fraction of the secret documents liberated by

Edward Snowden have been published or reported by the journalists he gave them to. While Glenn Greenwald and his colleagues have been accused of everything from helping terrorists and paedophiles to profiteering and covering-up damaging information, they have been both judicious and responsible in the way they have released information. Moreover, the drip-feed of stories revealing the complicity of an ever wider group of companies and countries has ensured that one of the most important civil liberties stories of modern times has now been front page news around the world for more than six months. No other leak in history has managed this feat. "Highlights" of the NSA Files released so far include:

• The *Verizon* Court Order: the first of the Snowden leaks revealed that the NSA was collecting the phone records of millions of Americans. While the scheme was launched by the Bush administration, it was widely believed that Obama had scrapped it.

• "Prism": enables the NSA and GCHQ to "mine" information from the servers of some of the biggest American technology companies (*Google, Apple, Microsoft, Facebook, AOL, PalTalk and Yahoo*). A similar programme called "Muscular" was intercepting millions of records a day from *Yahoo* and *Google*.

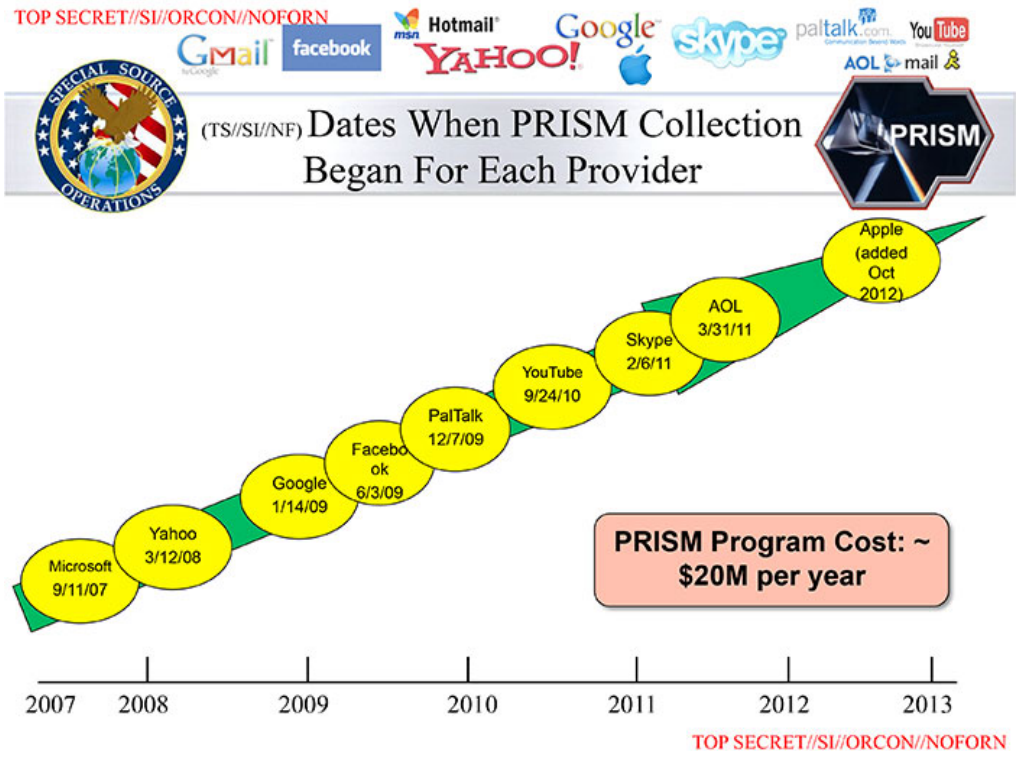
• "Tempora", part of the "master the internet" programme: GCHQ intercepts and stores the vast amounts of data flowing in and out of the UK via the undersea fibre-optic cables that are the veins of the World Wide Web. Similar "bulk-intercept" programmes are run by the NSA ("Blarney", "Fairview", "Oakstar" and "Stormbrew").

• "Xkeyscore": an NSA run data-retrieval system used to access emails, telephone calls, internet usage records and documents transmitted over the internet

• "Boundless informant": a data analysis and visualization system that provides an overview of the NSA's surveillance activities by country or program. Almost 3 billion "data elements" from inside the United States were reportedly captured by the NSA over a 30-day period ending in March 2013.

• "Bullrun" and "Edgehill": a $250 million-per-year programme under which the NSA and GCHQ (respectively) have defeated much of the encryption technology that underpins the security of the internet.

• Cyberwar, espionage and collusion: further revelations detail the extent to which the US is prepared to use international cyber-attacks to "advance US objectives around the world", the monitoring of phone calls of 35 foreign leaders and the complicity in NSA-GCHQ surveillance of intelligence services of –among others – Belgium, Denmark, France, Germany, Italy, Japan, the Netherlands, Norway, Singapore, South Korea, Spain and Sweden.




Source: NSA Slides, Washington Post, June 2013

## "By any means possible"

As Snowden explained from the outset, this baffling array of secret surveillance programmes demonstrates the lengths that the "intelligence community" will go to "obtain intelligence wherever it can by any means possible".

Entire communications networks are being placed under surveillance, whether "lawfully" (in the sense that access to the data they carry is a legal requirement of sanctioned by warrants that offer limitless discretion), under "voluntary" cooperation arrangements (between spy agencies and the companies that own those networks), or through state sponsored "hacking" (interception of the fibre-optic cables and data centres that host those networks).

The NSA has also been building "backdoors" into the applications and software of some of the world's largest IT companies and using malicious software to steal information from private, government and business networks. A recent document suggested that the NSA has "infected" more than 50,000 computer networks worldwide.

Together, the NSA and GCHQ have also compromised the cryptography that enables the transmission of information securely across much of the internet. Tim Berners-Lee, inventor of the World Wide Web called their endeavours "appalling and foolish" because they would "benefit criminal hacker gangs and hostile states", adding that he was "very sympathetic to attempts to increase security against organised crime, but you have to distinguish yourself from the criminal".

Unless you believe that the activities outlined above are entirely appropriate things for democratic governments to be doing, Edward Snowden's actions are the embodiment of principled whistleblowing and we owe him a huge debt of gratitude. That he has been forced to seek asylum in Russia, not just from the USA but its European partners, some of whom showed unprecedented contempt for diplomatic convention in grounding the plane of the President of Bolivia to look for him, shames all concerned and speaks volumes about the values and interests of Western governments today.

## "Big data", bigger problems

In considering how surveillance fits into the current state of power, what has completely changed since the likes of the Stasi had entire populations on file is that a privately-owned infrastructure has become the frontline of intelligence gathering. In turn, mass population surveillance is no longer the preserve of totalitarian regimes but a staple of democratic ones.

The revolution in information and communications technologies (ICTs) is transforming our relationship with everyone and everything. As more and more of our relationships move online – our interactions with friends and acquaintances on social media, with businesses and service providers through "e-commerce", with banks and "e-government" services and with political campaigns – more and more information about us is collected. Everything is recorded, stored and analysed. The economic and organisational rationale for keeping this data forever grows stronger every year.

What we do in the digital world betrays our thoughts, interests, habits, traits and characteristics. And as a species it turns out that we are entirely predictable: "embarrassingly so", according to a former General Counsel of the NSA. As more and more of the things we own are connected to the digital world, and more and more online services are provided for us, the more sensitive and complete the information we commit – where we were, what we did and who we did it with.

We leave this data everywhere. It includes personal data (information identifying us), content data (what we write and say) and "metadata" (data about data, such as call records, internet traffic, location data etc.). Many digital innovations rest on the collection and analysis of this information, from the maps on our "smart phones" to the many applications through which information and culture is shared and consumed. The need to protect ourselves from intelligence and security agencies bent on circumventing our rights to privacy is thus only part of the problem. We also need to make sure we are protected from those companies whose bottom lines depend on accessing (and monetarising) as much of our personal information as possible.

These twin problems are exacerbated by a third: "big data", less a concept than the marketing shorthand that encapsulates a new industry: *Have a large dataset? We can help you understand your clients, customers, employees, networks, threats, risks, opportunities etc.* This is where the "dark side" of ICTs – what Naomi Klein so accurately described as the "merger between the shopping mall and the secret prison" – is at its most obvious. The very same algorithms and analytical tools that Facebook uses to understand your interests and desires, and *Amazon* uses to calculate (and miscalculate) what else you might like to buy, can be used by government and private security companies alike to calculate (and miscalculate) whether you may be a threat, now or in the future. And it is precisely the "dual use" nature of this technology that makes it so hard to regulate. *It's not a surveillance*

*system, it's a data analytics suite* is the narrative behind the thriving international trade in truly Orwellian tools.

Problematising the surveillance revealed by Edward Snowden is relatively straightforward. Security and intelligence agencies running amuck across an insecure digital infrastructure using unchecked powers inherited from the analogue age, to paraphrase *Human Rights Watch*. Achieving meaningful reforms that properly address this problem is a much more difficult proposition because of the vested interests in maintaining the status quo and the jurisdictional issues that arise in any attempt to restrict transnational surveillance networks. These problems are compounded by profound changes in the relationship between people, states and corporations.

## Silicon Valley vs the NSA?

In December 2013, eight of Silicon Valley's most successful technology firms – *Aol, Apple, Facebook, Google, Linkedin, Microsoft, Twitter and Yahoo* – called for "wide-scale changes" to US government surveillance based on five principles for reform: (i) "sensible limitations" on government collection of information and an end to bulk data collection, (ii) stronger oversight and accountability of intelligence agencies, (iii) transparency about government demands and surveillance powers, (iv) respect for the "free flow of information" and (v) a "robust, principled, and transparent framework" to govern lawful requests for data across jurisdictions.

This initiative builds on earlier, tentative steps toward greater surveillance transparency, in which some of these companies have been publishing comparative information about government and law enforcement agency demands for their users' data and petitioning the US government to let them publish some of the information about their hitherto secret dealings with the NSA. It is notable that fixed line and mobile telephony companies, many of which have been unquestioningly facilitating state surveillance for much longer than their web-based counterparts, have not weighed in to the debate in the same way; though they never claimed to be pro-democracy either.

That nothing apparently stirred the White House into action more than the concern that the revelations had been particularly damaging for some of the USA's most valuable corporations speaks volumes about the state of power. But it also begs broader questions about how corporate power is exercised. Some of these companies have (to significantly varying degrees) been or become proactive in pushing back on state surveillance, but some of them have also been fiercely resistant to draft legislation designed to give individuals greater control over what happens to the personal data that their profit margins depend on, including provisions with the draft EU Data Protection Regulation.

*We will help protect you from government surveillance but you don't need protecting from us* is quite a proposition for a group of companies who, according to *Forbes*, spent more than $35 million on lobbying activities last year. *Google* alone accounted for just over half of this total ($18.2 m); if trade associations and lobby groups are excluded only *General Electric* admits to spending more on lobbying (*Microsoft* ($8.1 m), *Facebook* ($3.9 m), *Yahoo* ($2.8 m) and *Apple* ($2 m) make up almost all of the rest of the $35m).

There can be little doubt that these companies are genuinely opposed to the kind of dragnet surveillance and data warehousing being conducted by the NSA because it is a genuine threat to their bottom line. As *Microsoft's* General Counsel put it: "People won't use technology they don't trust. Governments have put this trust at risk, and governments need to help restore it". But as their top people head off to Davos to demand better transparency and oversight of surveillance in the name of preserving the "integrity of the internet", we should be asking what else they seek and receive of our leaders and legislators. We should also be asking the European technology sector where it stands on surveillance reform, and why it hasn't stepped up to the plate.

## Europe vs the "Great Satan"?

Public outrage at the Snowden revelations is such that there is now significant political capital bound up in surveillance reform. But the considered criticism and demands for change heard from Angela Merkel and Barack Obama have not, at least as yet, been matched by political action. Indeed, cosmetic reforms notwithstanding, there is little evidence of of appetite for the deeper structural changes to the deep state that are so obviously required.

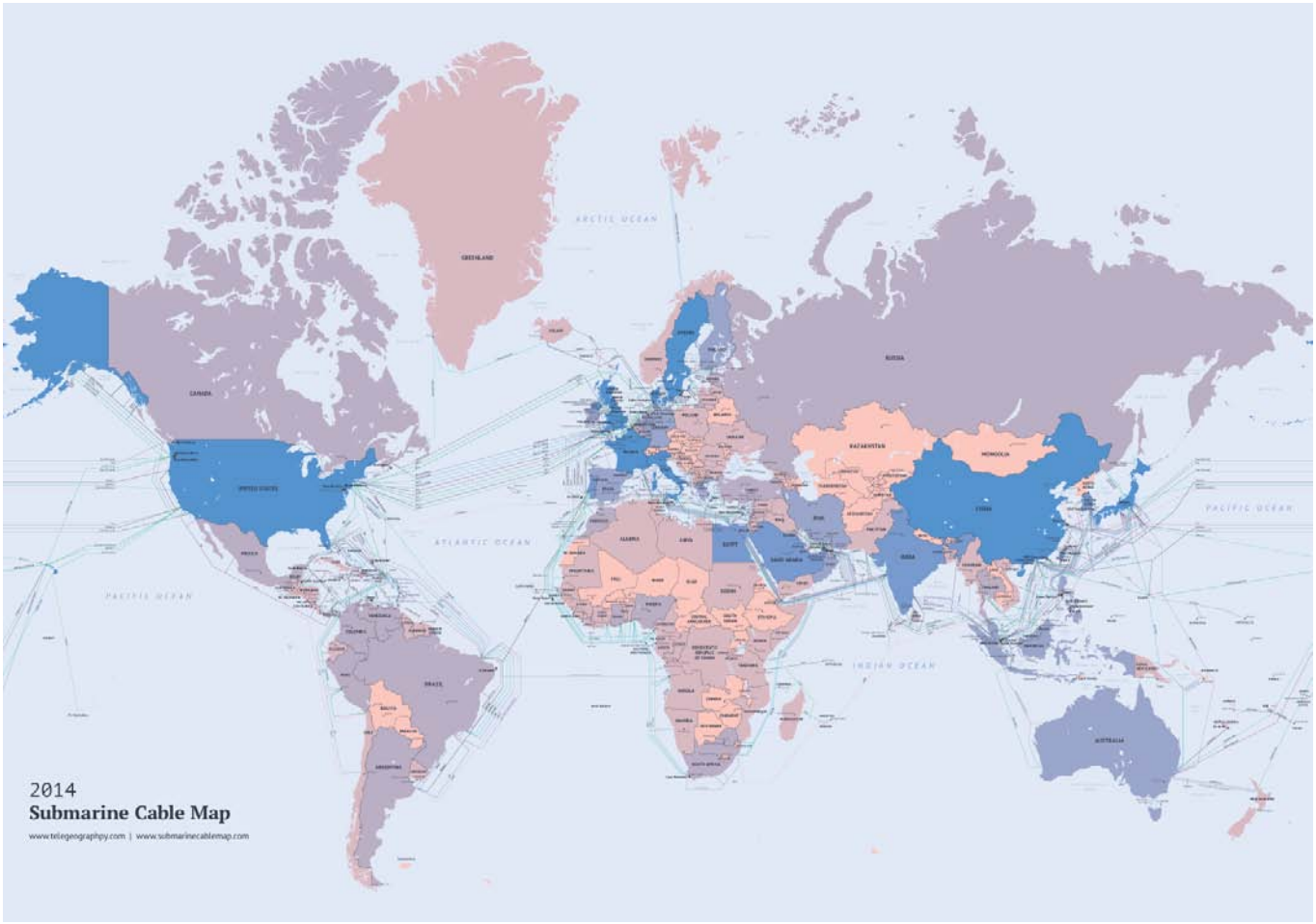
EU governments adopted a joint statement criticising their Transatlantic partner and warning of a collapse in trust, but have not threatened further sanction. Vocal in their criticisms of the USA and UK's activities, European governments have simultaneously sought to ensure that the activities of their own national security and intelligence apparatuses are kept out of the debate. Angela Merkel, the German Chancellor, has done a great job of playing to the domestic crowd (NSA "like the Stasi", "friends don't spy on each other" etc.) while largely ignoring widely held concerns about domestic surveillance and dispatching a team of negotiators of

Washington in what looked primarily like an attempt to secure Germany's admission to the "Five Eyes" club. In cahoots with the UK, the German government also blocked the swift adoption of the draft EU Regulation on data protection requested by the EU's Parliament and Commission, stalling long debated and much needed reforms.

The French government described the NSA's practices as "totally unacceptable" before including provisions in the Defence Bill 2014-2019 that grant its own intelligence services expanded powers to record telephone conversations, access emails, location and other "metadata" – with no judicial oversight whatsoever. Meanwhile the UK government, whose spying on its EU partners surely represents a transgression against "friends" of a far greater magnitude than anything the USA has managed, has been the most brazen in rejecting any criticism, describing GCHQ's critics as "airy-fairy" types and encouraging a witch hunt against the Guardian. This has seen Glenn Greenwald's partner detained at Heathrow airport under-terrorism laws and a laptop owned by the newspaper destroyed with an angle-grinder under supervision of state agents. None of this bodes well for the state of democracy in that country.

The European Commission, devoid of any power whatsoever as regards EU member states' national security policies, has been very outspoken about the NSA's spying, but has in practice been reduced to threats and finger-wagging in the direction of Silicon Valley, which is a bit rich since some of Europe's own communications surveillance arrangements are just as problematic. The EU Court of Justice has just indicated that it will likely quash a Directive, championed by the Commission, that mandated telecommunications and large internet service providers to keep metadata for 24 months for law enforcement and security purposes, because it failed to provide for adequate judicial oversight (or indeed to stipulate any meaningful restrictions on access to the data).

The European Parliament has just completed an enquiry into the surveillance of EU citizens by the NSA and their European counterparts, but in the absence of the power to compel witnesses to testify has relied on journalists, campaigners and independent experts. Its draft recommendations, which are not binding on the EU, will likely include the suspension of several data sharing agreements with the USA until it provides reciprocal privacy and data protection rights, the development of an "EU cloud" and reform of European mass surveillance programmes.




Telegeography 2014

As to the USA, for all the opining on the terrible state of democracy in that country, it is already streets ahead of EU member states in considering the domestic reforms that maybe necessary to safeguard its citizens' against intelligence "overreach". A Federal judge has just produced a preliminary ruling stating that the NSA's bulk phone record collection is likely to be in violation of the US constitution, also labelling the practice "indiscriminate", "arbitrary" and "almost-Orwellian". This sentiment was then echoed by a Presidential 'Review Group on Intelligence and Communications Technologies' whose 46 recommendations – if implemented in full – would at least lead to some significant curbs on the NSA's surveillance powers.Time will tell if Obama is up for the fight; the historical precedents are not encouraging.

## International law vs. (trans)national security

Whether we live in the kind of world where the NSA and its allies can do whatever they want to the internet and the secrets it holds or whether we don't really comes down to how much respect we have for the rule of law and the principle of universal human rights, in particular the right to privacy – a right on which many other rights depend. As Edward Snowden put it: "I don't want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity or love or friendship is recorded".

Limits to "domestic" spying powers are relatively straightforward in the context of national constitutions which should afford citizens clear rights to privacy and protections from undue interference from the state. What is much more problematic is that nationals of other countries – who do not usually enjoy the same rights of citizens – can easily be subject to surveillance by a foreign state.

This is crucial for two reasons. First, digital communications frequently pass through the territory or jurisdiction of foreign countries, particularly the USA, where the majority of the world's internet traffic is destined. This means that if you are not a citizen of the USA, any constitutional right to privacy you might enjoy in your own country is likely all but worthless as you traverse large parts of the internet. Second, while the main protagonist in the NSA Files is of course the USA, that agency is at the centre of a still highly secretive and almost entirely unregulated transnational intelligence network with a global reach. This is why, as *Privacy International* has undertaken, opening up the "Five Eyes" is a prerequisite to meaningful restriction of its powers.

Obama's review panel surprised some by recommending that the surveillance of non-US citizens be subject to be stronger oversight and that their right to privacy be recognised, but it effectively ruled out judicial protection for the individual subjects of foreign surveillance and proposed a lower threshold of "reasonable belief" (rather than probable cause) for surveillance required in the interests if national security. Neither would persons outside the USA benefit from the proposed obligations on the NSA to minimise the data held on US citizens.

This is unlikely to satisfy European critics of the USA's practices or the likes of the Brazilian government, which is demanding that all foreign telecommunications service providers operating in Brazil host their servers in that country so their citizens' data is only subject to Brazilian law. With other countries threatening to go the same way, it's not just companies who are warning against "Balkanisation" of the internet as current norms and technical standards are pulled apart.

While the "Summer of Snowden" demonstrated the power of the NSA and the big tech companies, it has also shown up the weakness of international law and the current system of international governance. Human rights law and jurisprudence leaves little room for doubt that what the "Five Eyes" and others have been doing contravenes both the letter and spirit of international law. It is not just human rights standards that have been ignored, but decades of carefully crafted mutual legal assistance frameworks (allowing states to request and access information or evidence about one another's citizens), some of which have been simplified since 9/11.

Advocates of global governance should be crying out for international agreements that both limit surveillance and enshrine individual rights to privacy and due process, but it is currently inconceivable that states will accept any international treaty that seeks to limit their national security capacities. The "big data" corporations can also be counted on to resist any attempt to codify the right to privacy or data protection into international law. For all the talk of surveillance reform, it is notable that the Silicon Valley principles make no mention of whatsoever of individual rights, digital or otherwise.

Nevertheless there is tangible and growing support for such measures. The United Nations General Assembly has just adopted a ground-breaking Resolution (proposed by Germany and Brazil) on "The right to privacy in the digital age", though it is only binding on the UN's High Commissioner for Human Rights, who will be instructed to prepare a report on the matter. A new optional protocol to the International Covenant on Civil and Political Rights (ICCPR) has also been suggested, but, even if the political

can be mustered, it will at best take years to agree and much longer to ratify. In the short term, domestic measures that limit surveillance by intelligence agencies are the only meaningful route to reform.

## Needles vs haystacks

Edward Snowden's revelations have already inspired a growing number of legal challenges and courts in Europe and the USA are being asked to weigh the legitimacy of what has been revealed against legal requirements to respect human rights and due process. This is the latest incarnation of the decade-old debate about the need to balance "liberty" with "security" and the new practices introduced under the "war on terror". It is a debate that liberty has been long been on the losing side of; it must be hoped that Snowden has reversed this trend. In the political arena, it has taken the form of a struggle against mass, indiscriminate surveillance and in favour of laws mandating surveillance only when necessary, targeted and proportionate.

What both of these debates too often ignore is the fundamental shift in what "national security" now entails, from the labour intensive, record-keeping era of Hoover and McCarthy to the banks of "big data" and intensive processing that NSA boss Keith Alexander now presides over. In this sense the power struggle is between a 20th century set of liberal democratic checks and balances, grounded in nation states and the regulation of investigatory powers, and a new transnational, pre-emptive and mass surveillance-based model that has developed in the 21st. The difficulty in trying to make this new model respect traditional notions of probable cause and due process is that the many of the methods it uses are antithetical to these notions.

Pre-emption has long been at the core of the state's national security mission. Whereas surveillance by police investigating criminal activities is supposed to start with "probable cause" that a known suspect is worthy of attention followed by judicial authorisation for any intrusive measures, national security agencies are essentially tasked with identifying threats and mitigating risks before they materialise. Post 9/11, this risk management paradigm has spread throughout the "Homeland Security" apparatus to encompass everything from pre-emptive detention to secret blacklists and extrajudicial killings by drone strikes, fuelling state repression across the world and encouraging the targeting of anyone who challenges the *status quo.*

Forced to defend their bulk data collection programmes for the first time, intelligence chiefs have repeated the same mantra over and over again: "we need the haystack to find the needle". Consequently it is argued that any push back on surveillance compromises national security. While this provides a convenient defence of mass surveillance, the reality is that police and intelligence service alike have long had access to the "haystack" on a case-by-case or even blanket basis; what Snowden has revealed is the construction of giant haystack comprised of as much historical data as possible that allows the NSA and its allies to literally rewind to what their citizens have been doing at given points in time.

The first test for meaningful surveillance reform, therefore, is to end the bulk collection of data by intelligence agencies. Given the culture of surveillance among hundreds of thousands of state agents and contractors, and the infrastructure NSA has invested in to facilitate this mass surveillance (it has just constructed one of the largest data storage facilities in the world in Utah), we should not underestimate the enormity of this task. The second test is to prevent large datasets – not just communications metadata but financial data, travel data, health data and so on – being accessed by state agencies in the absence of a legitimate reason for doing so and effective vigilance of those requests. If we are to protect the presumption of innocence and right to privacy in a big data environment then ultimately we need firewalls that both limit profiling and prevent "fishing expeditions" devised to identify grounds for suspicion among the innocent.

The third is to circumscribe the conditions under which intelligence security agencies can access this data to fulfil their mandates. This challenge requires both greater transparency on the part of those doing the surveillance (we need to know how the "haystacks" are being used in practice and by whom) and a much clearer distinction between matters of national security on the one hand and criminal intelligence gathering on the other. This is really a question about how much of the "war on terror" should be conducted by secret intelligence and military agencies and how much should be prosecuted within a rule of law framework. The fourth challenge is to replace the cosy, pro-establishment parliamentary committees currently tasked with oversight of these agencies with meaningful forms of democratic control.

Ultimately, the current needle/haystack debate hinges on how much if any data should be retained by the companies that hold or carry it for law enforcement and security purposes and the circumstances under which it can be accessed. Danger lies in the smoke and mirrors that could normalise what exists instead of scaling back what has been revealed. Obama's NSA review panel

proposed an end to the bulk metadata collection by the NSA, but proposed instead that service providers keep it for 30 months with access to the data controlled by the (traditionally permissive) surveillance courts.

As noted above, the EU may be moving in the other direction; its Court of Justice's advisory opinion having adopted a dim view of its "Data Retention Directive" and the principle of keeping data for long periods just in case it later proves useful for police and security agencies. Ultimately the two sides will have to resolve at least some of their differences in respect to surveillance powers and privacy protections if existing EU-US cooperation is to be maintained or deepened. This may even offer the best prospects for the substantive development of an international agreement in the longer term.

## The state within the state we're in

Near the top of the list of most post-Snowden demands for surveillance reform are better oversight and accountability of the intelligence services. But given the lack of political will to fundamentally appraise how liberal democracies have allowed their intelligence apparatuses to become so extraordinarily powerful and unaccountable, this is a huge ask. As one former UK judge wrote after the Snowden leaks, "The security apparatus is today able in many democracies to exert a measure of power over the other limbs of the state that approaches autonomy: procuring legislation which prioritises its own interests over individual rights, dominating executive decision-making, locking its antagonists out of judicial processes and operating almost free of public scrutiny".

This is what campaigns for surveillance reform are up against and it is naïve to think that demands for surveillance accountability will naturally succeed where a decade of trying to hold the USA and its allies to account for their roles in extraordinary rendition, torture, secret detention, internment and war crimes under the "war on terror" have met with such resistance (not to mention the criminal conduct that goes much further back than 9/11). Across Europe and North America in inquiry-after-inquiry, proceeding-after-proceeding, the law has frequently failed to provide redress as states have closed ranks and governments have adopted the default position of defending, ignoring or exonerating the actions of their intelligence and security agencies. Why? Because their national security and foreign intelligence apparatuses are intimately involved in everything states do militarily and in a good deal of their foreign and economic policies and interests. In geopolitics, surveillance capabilities – or "situational awareness" – is at the very heart of the projection of hard and soft power.

There is another fundamental issue with many of the current calls for surveillance reform. That is at some point trying to retrofit checks-and-balances on surveillance agencies that work in secret to pre-empt "threats" from enemies known and unknown inevitably becomes a contradictory exercise: taken to its logical conclusion, the argument that all surveillance must be necessary, proportionate and under proper democratic and judicial control is really an argument for radically restricting the mandate and powers of the intelligence services and tasking police and criminal intelligence services with problems like terrorism instead. Thanks to the cult-like obsession with (in)security across the majority of our media, this is akin to blasphemy.

Perhaps this is why so many campaigners talk about surveillance as if it occurs in a vacuum, ignoring the staggering development of national security apparatuses, particularly since 9/11, their impact on "suspect communities" and their relationship to strategies to combat "radicalisation" and "domestic extremism". Brown is the new Black and Green is the new Red. Across the world the kinds of peaceful protest and civil disobedience that democrats profess to cherish is under attack like never before with those who (logically) advocate more peaceful direct action cast as "extremists", even "terrorists". The struggle against unchecked surveillance should be at the heart of struggles for social justice.

We might also ask how it is that neoliberalism has successfully captured so many public services through the rubric of waste and efficiency, while the High Priests of the Security States can spend countless billions on armies of contractors and facilities designed by Hollywood-set makers at will? Having recently attended "MILIPOL", the 18th "Worldwide exhibition of internal state security" in Paris, I find it harder than ever to avoid the simple conclusion that it is because what is good for the security state is good for business, and vice versa.

"Homeland security", most of it centred in some way or another on mass surveillance techniques, is already a multi-billion dollar business. With it comes an increasing blurring of the boundaries between military force, national security and public order and the mania for everything from drones to "less lethal" weapons, crowd control technologies, mass surveillance applications, militarised border controls, and everything else on show at MILIPOL (see further TNI and Statewatch's Neoconopticon report of 2009). I wonder how many of the big players will now be at Davos, using fear and insecurity to sell what, in the show room, looks a lot like the powerful trying to protect themselves from the powerless.

The Emperor has designer clothes and designer

armour. It must be assumed that an already powerful surveillance industry will seek to fill any "security" void created by the democratic control of state surveillance. If we're serious about limiting surveillance, we need serious restrictions on state and private sector alike.

## Power and autonomy under digital capitalism – from rights to currency?

Globalised, mass surveillance has emerged because the international agreements designed to prevent the emergence of authoritarian states in Europe in the wake of the World War II have failed to check the consolidation of precisely this kind of illegitimate power, particularly since the end of the Cold War. Bodies like the EU and UN, captured by corporations or small numbers of powerful states, have inadvertently accelerated these processes. The "big data" controllers have secured all the rights and all of the information. Privacy has become something you opt-in to: by shunning some services and availing yourself of others. There is market for this kind of "security" too, it just doesn't yet enjoy the government support and public subsidies that the security industry gets.

Astute contrarian Evgeny Morenov, writing recently in the *Financial Times*, criticised the narrow focus of debates about "intelligence overreach", arguing that everyone including Snowden himself has missed the key point about the world of mass surveillance he revealed: "the much more disturbing trend whereby our personal information – rather than money – becomes the chief way in which we pay for services – and soon, perhaps, everyday objects – that we use?".

It's long been the case that if the service is free *you are the product*, but as consumers serve up more and more personal data in return for social capital and material gain, the greater the potential for those who control the "big data" to influence their fates in ways we don't yet recognise – a premise which is profoundly undemocratic in its own right. For Morenov, this is a "new tension at the very foundations of modern-day capitalism and democratic life". He is right that "a bit more imagination" is needed to resolve it.