Afterword: Securing freedom

Obama, the NSA, and US foreign policy

Andrew Hammond and Richard J. Aldrich

> Throughout American history, intelligence has helped secure our country and our freedoms (Barack Obama, Remarks on the Review of Signals Intelligence, 17 January 2014).

Introduction

In October 2013, Europe witnessed a diplomatic furore. The German magazine *Der Spiegel* revealed that America's largest spy agency, the National Security Agency (NSA), was intercepting data from the mobile phone of Angela Merkel, Germany's Chancellor. The subject dominated the EU Summit that began on 24 October and the American ambassadors to Berlin and Paris found themselves besieged by embarrassing questions they would rather not answer. Although many former intelligence practitioners dismissed the uproar as 'crocodile tears' – explaining that the Germans also conduct extensive electronic espionage – the political fallout was considerable. 'Spying between friends, that's just not done,' Merkel told the summit. 'Now trust has to be rebuilt' (Spiegel Staff 2013).

The source of these revelations was the former NSA contractor, Edward Snowden. His documents and PowerPoint slides have made the headlines weekly since June 2013. Yet as of January 2014, less than one per cent of his material had been released. Recognizing the possibility of repeated embarrassment, Obama had already ordered a number of internal reviews and inquiries. These revealed that Merkel was not alone. According to the *Wall Street Journal* the NSA – America's pre-eminent signals intelligence agency – had routinely monitored some thirty-five world-leaders. Some of this surveillance was stopped abruptly, including operations against senior figures in the United Nations, the International Monetary Fund, and the World Bank. In December 2013, newly released documents from Snowden revealed a new range of surveillance targets that included the office of the Israeli Prime Minister and the leaders of major international companies and aid organizations (Appelbaum *et al*. 2013).

Further transatlantic embarrassment followed. Perhaps the most interesting figure on the surveillance lists was Joaquín Almunia, then serving as Vice President of the European Commission. Significantly, he enjoyed a watching brief over antitrust issues in Europe. The European Commission exercises significant powers in the realm of international trade and it has used these powers against American companies in the recent past. Microsoft and Intel, for example, have suffered large fines for impeding fair competition. The leaked documents indicate that NSA, together with its British partner GCHQ, intercepted Almunia's communications in 2008 and 2009 (Glantz and Lehren 2013). EU trade diplomacy is a sensitive subject and predictably perhaps, the European Parliament responded by declaring the activities of the NSA and GCHQ to be illegal (Hopkins and Traynor 2014). Evidence has also

emerged suggesting that the Americans joined with the British to spy on the Israelis, the Germans, and the European Union, or worked with the Canadians to spy on the Brazilians.

The White House has been forced to ask serious questions about the relative costs and gains of such ventures. On 17 January 2014, after a number of reviews and consultations that lasted six months, Obama announced a range of changes to practice and procedure. Although these changes were modest, the White House had been placed on notice. A series of whistle-blowers and leakers – of whom Edward Snowden is the most recent and most prominent – has created a climate of 'regulation by revelation' (Aldrich 2009). The details of any future secret intelligence programmes will probably have to be defended in public and this may very likely have a deterrent effect.

Yet, as Obama said in his January 2014 remarks on NSA reform:

> what is at stake in this debate goes far beyond a few months of headlines, or passing tensions in our foreign policy. When you cut through the noise, what's really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed (White House 2014).

Glen Greenwald, the *Guardian* journalist who acted as Snowden's conduit for the disclosures, concurred in a response to Obama's speech on CNN: 'the question really is what kind of values do we have as a country' (Greenwald 2014). As so often in American history, then, the central axis of contestation is over the fraught and ever-evolving relationship between two values that Thomas Paine took to be 'the true end of government': freedom and security (Paine 1995 [1776]: 7). This conversation has become charged of late as the result of the recent NSA disclosures, set against a background of accelerating technological change.

The NSA before Obama

Organizationally, intelligence derived from electronic interception – known in the trade as 'sigint' – has always belonged to the US military. Despite a history of diplomatic code-breaking success during the Second World War, the failure to predict the outbreak of the Korean War prompted Harry Truman to create a single sigint entity called the National Security Agency in November 1952. This approach was partly inspired by the British who had already unified their own interception programme around Government Communications Headquarters or GCHQ in the immediate post-war period. It differed in the fact that while GCHQ Directors tend to be civilians, every NSA Director – including the one that has mostly served Obama, General Keith B. Alexander – has been a senior military officer. Indeed, a 1971 Department of Defense Directive ensures that this is so. In the American system of government, nonetheless, singularity is never easy to enforce. The CIA and later the DEA, for example, have run their own parallel sigint programmes and it was a joint NSA–CIA field unit (the Special Collection Service) which carried out the tapping of Angela Merkel's phone (Cass 2003).

Since the end of the Cold War, the biggest enemy of the NSA has been technological change. Michael Hayden, NSA Director between 1999 and 2005, explained that while mobile phone usage had increased from 16 million users to 741 million, internet usage had increased from 4 million users to 361 million (Aldrich 2010: 486). This volume has continued to increase exponentially; with the world sending more than 3 million emails a second by 2014. Fibre-optic cables carried much of the traffic, but were difficult to tap into. Even if this tsunami of new electronic material could be collected and stored, analysing it seemed an

impossible task. Not only was the NSA budget reduced by 30 per cent due to post-Cold War retrenchment, but the changed international environment was also characterized by a proliferation of new security challenges and subjects of interest. These required a broader range of language skills and resources that were simply not available (Aid 2003).

During the 1990s, Hayden's predecessors were confronted with this need to address breath-taking change in the realm of information and communications technologies. Looking for radical changes in working practices, they turned to the private sector. Partnerships with large companies like Narus and Northrup Grumman delivered innovative approaches that allowed NSA to trawl the internet. Meanwhile privatizing many of NSA's logistical needs and back-office functions allowed them to work a degree of budgetary magic. Indeed, by 2007 more than half the intelligence community's budget went to outsourcing companies (Shorrock 2008). Booz Allen Hamilton was one of the major contractors that came to its assistance and one of its employees was Edward Snowden.

The 9/11 attacks added to NSA's problems, but in their wake brought a massive influx of additional resources. Under George W. Bush, the American intelligence community budget increased from 45 billion dollars a year to 75 billion dollars a year (Shane 2012). This is almost certainly a profound underestimation since the operations in Iraq and Afghanistan brought with them additional moneys that helped to boost reconnaissance and surveillance programmes (Belasco and Daggett 2004). The PATRIOT Act (2001) also loosened some of the requirements under which the NSA had been operating due to the Foreign Intelligence Surveillance Act (1978). After 9/11, then, NSA had two primary missions. The first was to support the wars in Iraq and Afghanistan and the second was to support the wider campaign against terrorism on a global basis. NSA's work on political and diplomatic targets often came a poor third as resources were squeezed by the need to support an increasingly kinetic 'War on Terror'.

NSA struggled to support two simultaneous wars waged in freedom's name in Iraq ('Iraqi Freedom') and Afghanistan ('Enduring Freedom'). Neither the NSA nor the cryptanalytic arms of America's three armed services were prepared for the insurgencies that would unfold in both theatres. Arriving in Afghanistan in late 2001, their multimillion dollar ears could initially hear frustratingly little when ranged against low-tech insurgents who utilized cheap Japanese walkie-talkies; this was augmented by a dearth of requisite linguistic capabilities (Aid 2012). It was the same story in the aftermath of the invasion of Iraq. As the insurgency gained momentum the NSA was unable to deliver the intelligence that American forces needed. This began to be reversed in 2004 with the construction of the first Iraqi mobile telephone network. Iraqi insurgents and foreign fighters made extensive use of this, making themselves vulnerable to monitoring by the NSA. Along with geo-location and biometrics, sigint made a major contribution to American success in the Battle of Fallujah in November 2004 (Aid 2009). More importantly, at a crucial juncture in the counter-insurgency campaign sigint contributed greatly to the bloody but ultimately successful struggle between American Special Forces and insurgents operating inside Baghdad during 2007–8. The seamless integration of signals intelligence and night raids ensured that bomb technicians were killed or captured faster than they could be replaced (Urban 2010).

While the Bush presidency witnessed multiple inquiries into intelligence failure, they focused on the lack of warning for the 9/11 attacks and the hunt for mythical Iraqi WMD. The CIA and FBI were heavily criticized, but the NSA escaped relatively unscathed. Nevertheless, fear of another 9/11-style attack, underpinned by Al Qaeda attacks in Madrid in 2004 and London in 2005, prompted the NSA and its allies to channel significant resources to counter-terrorism. As we have seen, the internet, the exponential increase in types and volumes of communication – including Skype – were a major problem for NSA.

This was amplified by the challenge-and-response nature of the war against Al Qaeda. A programme of military strikes, rendition, and incarceration degraded Al Qaeda as a functioning hierarchic organization and removed its capacity to command or support terrorist attacks with training or personnel. Accordingly, militant Islamic terrorism shifted to self-starters who radicalized via the internet. The pressure to look at small groups or even individuals embedded in the United States and Europe required more granular detail as the search shifted towards terrorists who were increasingly alert to the growing perils of electronic surveillance (Sageman 2008).

Since the 1990s, both terrorism and organized crime have required the NSA to look at people rather than states. The NSA understood that the organizations that held the most data on people were not intelligence agencies or even governments, but supermarkets, banks, airlines, and ISP providers. The new intelligence agencies of the twenty-first century included Google, Facebook, and every commercial organization that issued its customers with loyalty cards. Meanwhile, the majority of citizens on the planet now emit 'electronic exhaust fumes' as the result of their everyday activities. Collecting, storing, and analysing this information – unimaginable in its extent – became a high priority for the NSA. Progress was made with additional resources granted by Congress, resources that were subject to only limited oversight. In 2008, the NSA began to finalize its plans for a new Data Center. This 1.5 million square feet facility stores data from intercepted satellite communications and fibre-optic cables in Bluffdale, Utah. The facility had to be built there, as power grids on the East Coast simply did not have the capacity to supply it.

The NSA's Utah Data Center boasts an annual electricity bill of some $40 million – suggesting that the NSA has been processing a lot of electronic data. In the ever-evolving relationship between American security and American liberty a key problem for the NSA has been that American law is much stricter on the surveillance of its own citizens than of foreigners. These are complex problems for a nation 'who in order to form a more perfect union' provided for a 'common defense… [to]… secure the blessings of liberty' (US Constitution). Despite NSA Deputy Director[1] John C. Inglis' assertion that liberty versus security 'is a false question… a false choice, at the end of the day we must do both' (2013), there are undoubtedly difficult trade-offs and politically consequential choices.[2] These problems reared their head during the Obama administration.

The NSA and Obama

During his presidential campaign, Barack Obama promised to reconfigure the 'War on Terror'. He offered a counter-terrorism strategy that would be both more ethical and more effective. At one and the same time Obama offered to deepen Bush's commitment to counter-terrorism while backing away from both the physical excesses and Manichean rhetoric of his predecessor. There was much continuity on counter-terrorism, but Obama's new approach had two important elements – first, taking the war to Al Qaeda in a more focused way through a significant increase in drone strikes and special force raids (Becker and Shane 2012). This was dramatically underlined during Operation Neptune Spear on 2 May 2011, which led to the death of Osama bin Laden. Second, was a heavy investment in intelligence designed to ensure there were fewer major terror incidents, especially within the American homeland (McCrisken 2011).

During his election campaign, Obama had emphasized the importance of reconciling national security imperatives with American core values and constitutional propriety. Accordingly, when Obama took office in January 2009 he was required to address a number

of what were taken to be toxic legacies. One of these was Guantanamo Bay, which he promised to shut down, something which proved much more difficult in practice. The other pressing problem was an NSA intelligence programme codenamed 'Stellar Wind'. This was a controversial eavesdropping operation that involved the mass surveillance of millions of American citizens in collaboration with major telcom providers. The purpose was to search for increasingly elusive Al Qaeda cells that were suspected of continuing to operate within the United States. The programme involved collecting the call data of American citizens en masse within the United States and subjecting it to data mining. Remarkably, the programme was conducted from Vice President Cheney's office without seeking the authority of America's main authorization body for such operations, the Foreign Intelligence Surveillance Activity Court, also known as the 'FISA Court' (Risen and Lichtblau 2005).

'Stellar Wind' was authorized by Bush shortly after 9/11 on the legal basis of 'wartime powers'. White House lawyers claimed that these powers trumped constitutional safeguards designed to protect American citizens from mass surveillance. Most lawyers, including the Dean of Yale University Law School, are deeply dubious about these arguments. The decision of America's largest telecom providers to hand over telephone billing records to the NSA, moreover, now looks plainly illegal. The effectiveness of the programme is also questionable. Robert S. Mueller, the Director of the FBI, has conceded that leads from the NSA's 'Stellar Wind' programme were so numerous that his FBI field agents who had to follow them up called them 'Pizza Hut cases' – because so many seemingly suspicious calls turned out to be takeout food orders (Gellman 2011).

Like the drone operation he inherited, 'Stellar Wind' has not only continued but expanded under the Obama administration. It has been succeeded by four different NSA programmes that span the full range of electronic communications and also allow this data to be cross-mapped with information from banking and financial sources (Gellman 2013). The NSA's defence of its actions has been that the FISA Court often took several weeks to authorize surveillance, by which time terrorists have often switched their communication channels (NSA 2009). However, most people suspect that the scale of the operation would have shocked the judges of the FISA Court – which almost never turns down a government request for surveillance. Indeed, worries that the courts would eventually find the activity illegal were so intense that Congress was persuaded to pass special retrospective legislation to grant senior executives at companies like ATT and Verizon immunity from prosecution. A variety of lower courts have judged 'Stellar Wind' illegal and government has been forced to resort to state secret privilege in an attempt to quash further legal review. The controversial nature of this particular activity underpinned Snowden's decision to leak a wide range of material about NSA in 2013.

One the most important aspects of Obama's national security strategy has been a firm determination to make secret programmes more secret still, and to avoid further leaks. The story about illegal domestic wire-tapping was first revealed in outline by two American journalists, Jim Risen and Eric Lichtblau, in stories published in *The New York Times* as early as 2005. One of their sources appears to have been the NSA whistle-blower Thomas Drake. Obama, to be sure, has been even more energetic than Bush in seeking to use the courts to punish government whistle-blowers and to bring pressure to bear on journalists who work with them. Indeed he has launched more legal actions against the press and their inside sources than any previous American president (Harris 2012). This is underlined by the thirty-five-year sentence imposed on Bradley Manning, the source of the State Department cables obtained by Wikileaks, and the decision to charge Snowden with espionage.

The NSA is not only America's largest intelligence and surveillance organism. It also fulfils two other functions: information assurance and cyberwar. The NSA serves as

America's main government authority for information assurance, including the security of the national electronic infrastructure and the internet. Some have asserted that this additional defensive mandate results in a conflict of interest, even a degree of institutional schizophrenia. Those who seek intelligence prefer weak and vulnerable electronic systems, while those responsible for information assurance and secure commerce prefer robust electronic architectures. The fact that NSA is also home to US Cyber Command makes this contradiction even more visible (Herrington and Aldrich 2013).

Cyberwar has formed an important instrument of Obama's foreign policy. In March 2010, Obama reportedly approved Operation Olympic Games, the electronic sabotage of Iranian nuclear facilities in collaboration with Israel.[3] Using a virus known as 'Stuxnet', Obama launched one of the most advanced cyber-attacks. The White House saw this as the only way to dissuade Israel from a conventional strike on Iranian reactors. The attack was successful, leaping across the air gapped facilities at Natanz, and the malicious software stopped many thousands of Iran's centrifuges. However, over-ambitious programming by the Israelis caused Stuxnet to spread to computers beyond the Natanz facility. Stuxnet made its way from the laptops of Iranian engineers out on to the internet, making it available for scientists all around the world to examine. Stuxnet is therefore the one of the first examples of unintentional cyberweapon proliferation. Again, the Obama administration has demonstrated its security-mindedness. General James Cartwright, one of those close to the operation, has been subjected to a year-long investigation by the US Department of Justice examining the leak of classified information about Stuxnet to the American media (Sanger 2012).

Obama's enthusiasm for the cyberwar dimension of the NSA has wider consequences for US foreign policy. American determination to achieve superiority in terms of offensive cyber-operations is somewhat at odds with the priorities of many of its allies, including many leading European states, who have tended to emphasize defence and stronger information assurance. Many countries around the world believe the aggressive development of cyber-warfare capacities threatens the electronic infrastructure of all developed states, not least because of the possibility that those developing these dark arts might become disaffected. American commercial software companies are especially anxious about the NSA's exploitation of hard-to-find flaws in software, believing that it is costing them millions in lost sales. Diplomacy around these complex issues now constitutes a fraught and rapidly expanding area of activity for the State Department (Nagyfejeo 2014).

Obama and Snowden

The NSA's most pressing tasks under both Bush and then Obama have been supporting America's two foreign wars, together with counter-terrorism. Diplomatic intelligence has been a lower priority. Nevertheless, NSA operations against the politicians and diplomats of friendly states have provoked America's friends and allies for more than a decade. In early 2003, for example, the GCHQ whistle-blower Katherine Gun revealed an NSA request to increase spying on the non-permanent members of the UN Security Council and Mexico in the run-up to the Iraq War (Aldrich 2010: 521).

This theme was revisited in 2010 when Wikileaks disclosed thousands of secret State Department cables. These demonstrated that US diplomats had been tasked to collect a vast range of personal data from their foreign counterparts in order to promote electronic surveillance. Notably embarrassing was a State Department cable sent to US diplomatic missions in 2009 entitled, 'Reporting and collection needs: The United Nations' that was in effect an espionage shopping list. US Foreign Services Officers were asked to acquire cell phones

numbers, telephone directories, email listings, credit card account numbers, and even frequent-flyer account numbers of foreign diplomats. Indeed, several retired American diplomats from the Reagan era were shocked, commenting that this had not been State Department practice in the past (Stein 2010). Snowden's revelations about the NSA spying on Angela Merkel have merely exacerbated an already familiar area of discomfort for American diplomats.

The issue of spying on friends matters more for Obama than it did for Bush. Obama has made a high-profile commitment to change the style of American foreign policy, placing more emphasis on multilateralism, co-operation with allies, and the United Nations as an institution. As Obama told the UN General Assembly the year he took office: 'The United States stands ready to begin a new chapter of international cooperation, one that recognizes the rights and responsibilities of all nations. And so, with confidence in our cause, and with a commitment to our values, we call on all nations to join us' (White House 2009). Moreover, although Obama travels significantly less than his predecessor, the overall rise in the importance of summitry and face-to-face discussion in world diplomacy, especially on economic and trade matters, makes these revelations even more embarrassing (Lee and Hudson 2004). Finally, the latest disclosures involve multiple embarrassments because they have exposed the way in which Britain and Canada work with the NSA to spy on other allies, causing deep anger among America's close espionage partners like GCHQ.

Obama reacted to Snowden's revelations in two ways. First, he ordered a discreet diplomatic offensive. American diplomats have responded to the NSA scandal by quietly pointing out that European citizens are much more likely to be watched by their own governments than the NSA. France has an almost identical system that collects nearly all telephone calls, emails, and social media activity that come in and out of France. Like the American NSA, the UK, France, Germany, Spain, and Sweden have all developed the ability to tap into fibre-optic cables allowing them to collect vast amounts of data. The NSA and GCHQ have reportedly advised other European countries on the best way to create a permissive legal regime to facilitate this. New legislation approved by the French Senate allows the authorities to use surveillance to protect 'the scientific and economic potential of France' raising the possibility of spying on foreign businesses and trade negations (Richet 2014).

Second, Obama ordered a series of reviews and reports. Obama has also personally met with leaders from companies like Apple, Twitter, Yahoo, Facebook, Google, and AT&T to discuss the NSA's data-collection methods, recognizing that intelligence activity is no longer really owned by the intelligence agencies but instead by all the major corporations that do business over the internet. The centrepiece was an NSA review taskforce consisting of former counter-terrorism chief Richard Clarke, former CIA Deputy Director Michael Morell, University of Chicago law professor Geoffrey Stone, former Obama regulatory expert and legal scholar Cass Sunstein, and former Office of Management and Budget privacy director Peter Swire. This taskforce produced a constructive and thoughtful report of over 300 pages entitled 'Liberty and Security in a Changing World'.[4] The most substantive recommendation is that the phone companies, not the government, store American metadata. Metadata is the call data – who called whom from where and when – that is at the centre of the 'Stellar Wind' controversy. This recommendation, they argued, would bring the NSA closer to the UK's GCHQ and the situation created in Europe under recent EU legislation, but would not radically alter the NSA's permissions or capability (PRGICT 2013).

From the point of view of American diplomacy, perhaps the most radical suggestion is that the NSA should be broken up and civilianized. Obama's panel wanted to see responsibility

for cyber-security and also for cyberwarfare removed from the NSA, leaving it with only its core intelligence mission. However, Obama told the advisory panel in short order that the Pentagon would continue to own America's largest spying agency. They were also told that the Director of the NSA would also continue to head the Central Security Service and US Cyber Command (Hughes 2013). In January 2014 this was confirmed when Obama chose Vice Admiral Michael S. Rogers, a specialist in cyberwar, as the new director of the NSA (Sanger and Shankerjan 2014). The irony here is that Obama has not only rejected many of the recommendations of his own panel, but also suggestions for restraining surveillance which echo those he himself made as Senator only five years ago. The shift in Obama's policy on surveillance is demonstrable, as is the overall calculus between national security and individual liberty (McCrisken 2011).

Meanwhile Obama himself has spent a good deal of time pondering the Snowden problem. His national security team have warned him that this episode threatens not so much the end of privacy for the citizen but rather the end of secrecy for government. Contrary to much of the expectation that came with an election campaign built upon a message of 'hope' and 'change', Obama has been extremely active in attempting to maintain and even increase state secrecy. Nevertheless, in a world in which increasing numbers of American government officials and contractors have access to high volumes of top-secret data, more 'Snowdens' seem likely.

Obama, then, has multiple concerns. Snowden has undoubtedly degraded the effectiveness and allure of an intelligence system that is costing America and its closest allies an estimated $100 billion a year. Obama is also anxious that the next disgruntled former employee might not choose to go to the newspapers. Instead they might choose to sell vast volumes of personal data that the government has collected on American citizens to unscrupulous parties, either to foreign countries or criminal enterprises, perhaps even the Russian mafia. Complex and costly lawsuits would certainly follow.

What action has Obama taken? Over the last few months two White House officials from the National Security Staff have been busy reviewing NSA overseas targets to assess whether the risk of embarrassment when exposed is worth the policy gains to foreign policy. US officials have already acknowledged that spying on Merkel was no longer occurring. This was part of a broader review of US intelligence activities around the world by all US espionage agencies, including the CIA, with what White House officials have called a special emphasis on: 'examining whether we have the appropriate posture when it comes to Heads of State; how we coordinate with our closest allies and partners; and what further guiding principles or constraints might be appropriate for our efforts' (Reuters 2014).

On 17 January 2014, Obama outlined his new policy on the NSA. It offered little change and rejected the more substantive recommendations of his own advisory panel. The big issue for Obama was the successor to 'Stellar Wind', a programme that American courts have attempted to declare illegal but which, as mentioned above, has expanded under Obama. He undertook to consider placing American metadata under the control of the telecoms who owned it rather than the NSA, but underlined that he was not prepared to abandon the associated intelligence capability. The catch here is that the NSA's capability depends on pooling as many different types of electronic data as it can in one place. As with Obama's promise to close Guantanamo, this has the appearance of a vague assurance without a concrete solution. For the same reason, Obama refused to go down the road of requiring more use of national security letters from the FISA Court, since this would push the NSA away from wholesale data mining and back towards 'retail surveillance' focused on named individuals.

Obama also ignored recommendations from the American software and computer industry: that the NSA should not deliberately weaken commercial software, and that they cease exploiting flaws in software to mount cyber-attacks or surveillance. America's Silicon Valley was clear that they thought that Obama had not gone far enough (Guynn 2014). Obama likewise made some implausible assertions. For example, he insisted that the NSA does not spy to provide America with commercial advantage. Yet, previous Directors of Central Intelligence, notably James Woolsey, have asserted that this is one of the intelligence community's missions. Obama did at least offer an olive branch to foreign heads of state, assuring them that there would be a list of premiers that the NSA could not spy upon. But even this raises as many problems as it solves. Who will be on the list, who will be off the list, and who will know (Landler and Savage 2014)?

Conclusion

In his recent landmark speech on sigint reform Obama attempted to root surveillance and NSA activity within a broader American struggle for freedom. However, his approach to the NSA and the broader diplomacy of surveillance is consistent with the rest of his national security policy. Increased surveillance has been central to the American exit from Iraq and the prosecution of the war in Afghanistan. It has also been important in hitting Al Qaeda harder in Afghanistan, Pakistan, and the Arab Peninsula. Nonetheless, it is difficult to square NSA activity during his watch with his much-vaunted emphasis on core values, especially the collection and analysis of metadata that is almost certainly unconstitutional. It is also difficult to square the aggressive targeting of the personal communications devices of friends and allies with Obama's ambition for a more multilateral foreign policy. In a world of summits, more personal embarrassment looms for Obama and for any US ambassador in Europe.

America's approach to the NSA, we may conclude, continues to be dominated by a sense of exceptionalism. The surveillance of foreigners, whether mere citizens or premiers, is not taken to be of fundamental importance. More significant are constitutional issues around the legality of domestic wiretapping in a country where 'individual freedom is taken to be the well-spring of human progress' (White House 2014). A country, what is more, which was founded upon a deep mistrust of overweening government and ideas of individual rights enforceable against the collectivity.

In December 2013 a federal judge decided that that the NSA's collection of bulk phone data – which was done without FISA authorization – was unconstitutional. US District Court Judge Richard Leon asserted that the practice was a clear violation of the Fourth Amendment ban on unreasonable searches, adding 'I cannot imagine a more "indiscriminate" and "arbitrary" invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval'. A government appeal is expected. Once again, however, state secrets privilege is likely to be used to quash the ruling.

Nevertheless, Snowden himself saw this court ruling as justifying his actions. 'I acted on my belief that the NSA's mass surveillance programmes would not withstand a constitutional challenge, and that the American public deserved a chance to see these issues determined by open courts.' Snowden's judgement was that both Congress and the American courts had failed as regulators of the intelligence community and that he had no option other than to attempt what might be called 'regulation by revelation'. Yet this has not worked either. Whatever changes might result from Obama's recent review, they are likely to afford little additional protection from surveillance for anyone, whether inside or outside

America's borders (Hughes 2013). The conversation over security and freedom with regards to this issue, therefore, will continue: as will the debate which is much broader still and which has been continued for over two centuries – that over the nature and meaning of America and its relationship with the outside world as it goes about the business of securing freedom.

Notes

1 The highest-ranking civilian within NSA.
2 In an effort to assuage public discomfort, on 29 January 2014 NSA Director General Alexander appointed an 'NSA Civil Liberties and Privacy Officer', former Senior Director for Privacy Compliance at the Department of Homeland Security Rebecca Richards.
3 The precise date is unclear, but Kaspersky Labs estimate that Stuxnet was released in March 2010.
4 In the American context, as Eric Foner notes, 'freedom' and 'liberty' are quite often used interchangeably (1998: xiii).

References

Aid, M.M. (1999) 'The time of troubles: the US National Security Agency in the twenty-first century', *Intelligence and National Security*, 15(3): 1–32.

Aid, M.M. (2003) 'All glory is fleeting: sigint and the fight against international terrorism', *Intelligence and National Security*, 18(4): 72–120.

Aid, M.M. (2009) 'The troubled inheritance: the National Security Agency and the Obama administration', in Loch Johnson (ed.), *The Oxford Handbook of National Security Intelligence*, Oxford: Oxford University Press, 243–56.

Aid, M.M. (2012) *Intel Wars: The Secret History of the Fight against Terror*, New York: Bloomsbury.

Aldrich, R.J. (2009) 'Regulation by revelation? Intelligence, transparency and the media', in R. Dover and M. Goodman (eds), *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence*, New York, NY: Columbia University Press, 13–37.

Aldrich, R.J. (2010) *GCHQ: The Untold Story of Britain's Most Secret Intelligence Agency*, London: HarperCollins.

Appelbaum, J., Stark, H., Rosenbach, M., and Schindler, J. (2013) 'Berlin complains: did US tap Chancellor Merkel's mobile phone?', *Der Spiegel*, 23 October.

Bamford, J. (1983) *The Puzzle Palace: America's National Security Agency and its Special Relationship with GCHQ*, London: Sidgwick & Jackson.

Becker, Jo and Scott Shane (2012) 'Secret "kill list" proves a test of Obama's principles and will', *The New York Times*, 29 May.

Belasco, A. and Daggett, S. (2004) CRS Report RL32422, 'The administration's FY2005 request for $25 billion for operations in Iraq and Afghanistan: precedents, options, and congressional action', 22 July.

Cass, S. (2003) 'Listening in: are the glory days of electronic spying over – or just beginning?', *Spectrum IEEE*, 9 May.

Danger, David, E. and Shankerjan, T. (2014) 'NSA choice is navy expert on cyberwar', *The New York Times*, 30 January.

DeYoung, Karen (2011) 'Secrecy defines Obama's drone war', *Washington Post*, December 20.

DeYoung, Karen (2012) 'A CIA veteran transforms US counterterrorism policy', *Washington Post*, 24 October.

Foner, E. (1998) *The Story of American Freedom*, New York, NY: W.W. Norton.

Gellman, B. (2011) 'Is the FBI up to the job 10 years after 9/11?', *Time Magazine*, 12 May.

Gellman, B. (2013) 'US surveillance architecture includes collection of revealing internet, phone metadata', *Washington Post*, 16 June.

Glantz, J. and Lehren, A. (2013) 'NSA spied on allies, aid groups and businesses', *The New York Times*, 20 December.

Gorman, S. (2008) 'NSA's domestic spying grows as agency sweeps up data', *Wall Street Journal*, 10 March.

Greenwald, Glen (2014) 'Interview: The Lead With Jake Tapper', *CNN Transcripts*, 17 January 2014, http://edition.cnn.com/TRANSCRIPTS/1401/17/cg.01.html

Guynn, J. (2014) 'Silicon Valley's reaction to Obama's NSA reforms: not enough', *Baltimore Sun*, 17 January.

Harris, P. (2012) 'Drone wars and state secrecy – how Barack Obama became a hardliner', *Guardian*, 2 June.

Herrington, L. and Aldrich, R. (2013) 'The future of cyber-resilience in an age of global complexity', *Politics*, 33(4): 299–310.

Hopkins, N. and Traynor, I. (2014) 'NSA and GCHQ activities appear illegal, says EU parliamentary inquiry', *Guardian*, 9 January.

Hughes, B. (2013) 'Stakes rise for Obama's NSA review', *Washington Examiner*, 17 December.

Inglis, J.C. (2013) 'NSA/CSS core values with NSA Deputy Director, John C. Inglis', National Security Agency/Central Security Service, 10 January 2014 (available online at http://www.nsa.gov/about/values/core_values.shtml).

Johnson, T.R. (2009) *American Cryptology during the Cold War, 1945–1989*, *Vols 1–4*, Fort Meade, MD: NSA.

Jones, G.G. (2013) *Hunting in the Shadows: The Pursuit of Al Qa'ida since 9/11*, New York, NY: Norton.

Landler, M. and Savage, C. (2014) 'Obama outlines calibrated curbs on phone spying', *The New York Times*, 17 January.

Lee, D. and Hudson, D. (2004) 'The old and new significance of political economy in diplomacy', *Review of International Studies*, 30(3): 343–60.

Madsen, W. (1998) 'Crypto AG: the NSA's Trojan whore?', *Covert Action Quarterly*, 63 (Winter): 36–7.

Markoff, John and David E. Sanger (2010) 'In a computer worm, a possible biblical clue', *The New York Times*, 29 September.

Mazzetti, Mark (2103) *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*, New York, NY: Penguin Press.

McCrisken, Trevor (2011) 'Ten years on: Obama's war on terrorism in rhetoric and practice', *International Affairs*, 87(4): 781–801.

Nagyfejeo, E. (2014) 'Transatlantic collaboration in countering cyber terrorism', in T. Chen, L. Jarvis and S. Macdonald (eds), *Cyber Terrorisms: A Multidisciplinary Approach*, New York: Springer.

NSA (2009) ST-09-0002 Working Draft, Office of the Inspector General National Security Agency/Central Security Service, reproduced in *The New York Times*, 9 March.

Olcott, A. (2012) *Open Source Intelligence in a Networked World, Continuum Intelligence Studies*, London: Continuum.

Paine, T. (1995 [1776]) *Rights of Man, Common Sense and Other Political Writings*, New York, NY: Oxford University Press.

Preamble to the Constitution of the United States (n.d.) The National Archives (available online at http://www.archives.gov/exhibits/charters/constitution_transcript.html).

PRGICT (2013) 'Liberty and security in a changing world: report and recommendations of the President's Review Group on Intelligence and Communications Technologies' (available online at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf).

Reuters (2014) 'White House conducting detailed assessment of NSA's targets', 9 January.

Richet, J.L. (2014) 'New French surveillance law: from fear to controversy', *Computerworld*, 7 January (available online at http://blogs.computerworld.com/privacy/23326/new-french-surveillance-law-fear-controversy).

Risen, J. and Lichtblau, E. (2005) 'Bush lets US spy on callers without courts', *The New York Times*, 16 December.

Rodriguez Jr, Jose A. with Bill Harlow (2012) *Hard Measures: How Aggressive CIA Actions after 9/11 Saved American Lives*, New York, NY: Threshold Editions.
Rosenbach, E. (2012) *Find, Fix, Finish*, New York, NY: Public Affairs.
Sageman, M. (2008) *Leaderless Jihad: Terror Networks in the Twenty-First Century*, Philadelphia, PA: University of Pennsylvania Press.
Sanger, David E. (2012) 'Obama order sped up wave of cyberattacks against Iran', *The New York Times*, 1 June.
Sanger, David E. (2013) 'In cyberspace, new cold war', *The New York Times*, 24 February.
Sanger, David, E. and Shankerjan, T. (2014) 'N.S.A. Choice Is Navy Expert on Cyberwar', *New York Times*, 30 January 2014.
Scahill, Jeremy (2013) *Dirty Wars: The World is a Battlefield*, New York, NY: Nation Books.
Shane, Scott (2012. 'Shifting mood may end blank check for US security efforts', *The New York Times*, 24 October.
Shorrock, T. (2008) *Spies for Hire: The Secret World of Intelligence Outsourcing*, New York, NY: Simon & Schuster.
Spiegel Staff (2013) 'Embassy espionage: the NSA's secret spy hub in Berlin', *Der Spiegel*, 27 October.
Stein, J. (2010) 'Former State Department intelligence chief says spy orders unprecedented', *Washington Post*, 29 November.
Urban, M. (2010) *Task Force Black: The Explosive True Story of the SAS and the Secret War in Iraq*, London: Little, Brown.
US Government (2002) *The National Security Strategy of the United States*, Washington, DC: The White House.
White House (2009) 'Remarks by the President to the United Nations General Assembly', *The White House*, 23 September 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-to-the-United-Nations-General-Assembly
White House (2014) 'Remarks by the President on Review of Signals Intelligence', *The White House*, 17 January 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
Williams, C. (2001) *Explorations in Quantum Computing*, London: Springer, 507–63.

Further reading

M. Aid, *Secret Sentry: The Untold Story of the National Security Agency* (New York, NY: Bloomsbury, 2009).
M. Aid, *Intel Wars: The Secret History of the Fight against Terror* (New York, NY: Bloomsbury, 2012).
J. Bamford, *Body of Secrets: How NSA and Britain's GCHQ Eavesdrop on the World* (New York, NY: Doubleday, 2001).
J. Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to Eavesdropping on America* (New York, NY: Doubleday, 2008).
David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York, NY: Crown Publishers, 2012).