Full written formal statement by Mr Thomas Drake

==========

Thomas Drake Statement
European Parliament LIBE Committee
Brussels, Belgium
30 Sep 2013

Thank you to the European Parliament and the Civil Liberties, Justice and Home Affairs Committee for inviting me to speak before your critically important public hearings – and the challenge you collectively face regarding the National Security Agency's surveillance programs and their impact on your respective member countries as well as the privacy of citizens in my country and yours.

The fundamental issue before your Committee is a foreign government (often in league with the intelligence apparatus of other countries as well as cooperatinginternet, phone and data service providers), spying on you under the guise of protecting its own interests in the name of national security – a convenient constraint of monitoring and control especially when conducted in secret -outside the purview of law and public debate - while subverting your sovereignty.

I used to fly as a crypto-linguist on RC-135 reconnaissance aircraft in the greater European theater during the latter years of the Cold War. My primary target of interest was East Germany. The Stasi became monstrously efficient using surveillance to enable their pathological need 'to know everything' – their very operating motto. However, I never imagined that the US would use the Stasi playbook as the template for its own state sponsored surveillance regime and turning not only its own citizens into virtual persons of interest, but also millions ofcitizens in the rest of the world. Do we really want to become subject to and subjects of a secret surveillance state?

In a surveillance state everybody is suspicious and laws protecting privacy and citizen sovereignty are regarded as inconvenient truths bypassed in the name of keeping the rest of us safe and secure as justification for the wanton and surreptitious bulk copy collection and unbridled access to vast amounts of data about our lives. Unfortunately, this surveillance regime has now grown into a globe girdling system that has gone far beyond prosecuting terrorism and other international crimes and wrongdoing.

Your Committee faces the challenge of dealing with a secret hidden shadow surveillance state dissolving the very heart of freedom and liberty and our respective citizen rights and using this power to expand sovereign-free zones – even when it undermines the very fabric of society, breaks trust between nations and endangers the very mechanisms we use for commerce and trade.

This exceptionalism gives rise to an ends justifying the means mentality in violating the sovereignty of other nations and citizens far beyond the real threats we do face from those who would cause us real harm, but often exaggerating those very threats in public for access to all of our data behind the scenes.

When national security services are more than willing to deliberately compromise the very information technology services and protocols that so many citizens as well as commercial and private enterprises rely upon and enjoy for legitimate confidentiality, data protection, and security in order to conduct their day to day business, it becomes very difficult to maintain trust in those systems.

Nothing less than the very sovereignty of our citizens and states are at stake in the face of an unfettered surveillance state apparatus.

From the recent disclosures of Edward Snowden, the US government hasroutinely violated on a vast industrial scale the Constitutional protections afforded its own citizens, while also disregarding the internal integrity of other states and the fundamental rights of non-US citizens.

I know. Because I was eyewitness to the very foundations of a persistent surveillance state greatly expanded in the deepest of secrecy right after 9/11. I was there at the beginning.

While a senior official at the National Security Agency, I found out about the use of a top secret domestic electronic eavesdropping program that collected and accessed vast amounts of digital data (including phone numbers, e-mail addresses, financial transactions and more), turning the US into the equivalent of a foreign nation for the purposes of blanket dragnet surveillance and data mining – blatantly abandoning and unchaining itself from the Constitution and a 23 year legal regime enacted due to earlier violations of citizen rights by US government's use and abuse of national instruments of power against Americans in the 60s and 70s.

These secret surveillance programs were born during the first few critical weeks and months following 9/11, as the result of willful decisions made by the highest levels of the US government. Such shortcuts and end-runs were not necessary, as lawful alternatives existed that would have vastly improved US intelligence capability with the best of American ingenuity and innovation, while fundamentally protecting the privacy of citizens at the same time.

I raised the gravest of concerns through internal channels, spoke directly with the NSA Office of the General Counsel, and then became a material witness and whistleblower for two 9/11 congressional investigations in 2002, and thenexposing massive fraud, waste, abuse and mismanagement at NSA during amulti-year Department of Defense Office of Inspector General audit from 2003-2005 regarding a multi-billion dollar NSA flagship intelligence collection programunder development that was far more costly and far less effective in supporting critical intelligence requirements than a readily available and privacy protectingalternative.

I followed all the rules as a whistleblower until it fundamentally conflicted with my oath to uphold and defend the Constitution, and made a choice in 2006 to exercise my First Amendment rights and went to the press with criticalinformation about which the public had a right to know regarding the fraud, waste and abuse as well as the secret and unconstitutional surveillance programs.

However, rather than address the illegality and wrongdoing, the government made me a target of a huge federal criminal "leak investigation" into the exposure of the secret surveillance programs and subjected me to severe retaliation, reprisal and retribution that started with forcing me out from my job as a career public servant. I was subsequently blacklisted, no longer had a stream of income, while simultaneously incurring substantial

attorney fees and other huge costs,necessitating a second mortgage on my house, emptying of my bank accounts, including retirement and savings.
What I experienced as a whistleblower sends the most chilling of messagesabout what the government can and will do when one speaks truth to and ofpower—a direct form of political repression and censorship.
And yet once exposed, these unconstitutional detours were (and still are)predictably justified by often vague and undefined claims of national security, while aided and abetted by shameless fear mongering on the part of the government.
And yet we are now in an era where sharing issues of significant concern in the public interest, which do not in any way compromise national security, are oftennow considered criminal acts of espionage aided and abetted by reporters and the press - yet anathema to a free, open and democratic society.
I did everything I could to defend the inalienable rights of all U.S. citizens and the sovereignty of the individual which were so egregiously violated and abused by my own government—when there was no reason to do so at all, except as an excuse to go to the proverbial 'dark side' by exercising unaccountable, irresponsible and "off the books" unilateral executive power in secret.
I blew the whistle because I saw grave injustice, illegality and wrongdoing occurring within the National Security Agency. I was subsequently placed under intense physical and electronic surveillance, raided by the FBI in 2007 and two and half years later under the Obama Administration criminally charged under a 10 felony count indictment including five under the Espionage Act, facing 35 years in prison. The extraordinary charges that were leveled against me by the US Department of Justice are symptomatic of the rising power of the national security state since 9/11 and a direct assault on freedom of speech, thought, innovation, and privacy.
The government found out everything they could about me and turned me into an Enemy of the State. I became the first whistleblower prosecuted in the decades since Daniel Ellsberg, under the draconian World War I-era Espionage Act, a law meant to go after spies, not whistleblowers.
Having the secret ability to collect and analyze data with few if any substantial constraints – especially on people, is seductively powerful – and when donewithout the person's permission and in secret against their will – is the ultimate form of control over others.
When government surveillance of this magnitude hides behind the veil of secrecy, when it professes openness and transparency while practicing opaqueness and deceit, that's when citizens need to become very aware and wary of what the future might hold – when their very liberties are eroded and even taken away in the name of national security -- without their consent.
The fear engendered through the invocation of threats (real and imagined),creates a climate where rights are ignored as the unifying cause for obsessing over national security and the use of fear by the government to control the public and private agenda.

My criminal case is direct evidence of an out of control and 'off the books' government that is increasingly alien to the Constitution and democracy at home and abroad. The rise in this form of a contrary alien form of government assuming the shape of a national security state under surveillance evidences the all too distinct and historically familiar characteristics of an alarming 'soft tyranny' and is anathema to all forms of democracy.

As Montesquieu wrote, "No tyranny is more cruel than that which is practiced in the shadow of the law and with the trappings of justice: that is, one would drown the unfortunate by the very plank by which he would hope to be saved."

One could make the case that the government chose to make me (and others) targets as part of a much broader campaign against whistleblowers in order to send the strongest possible message about what the government can and will doto suppress dissent and speech it doesn't like.

And yet the United States' brutal and unrelenting crackdown on whistleblowers is outdone by the magnitude of what it is now trying to hide or continue as a result of the Snowden disclosures. NSA is not just eavesdropping on all Americans and building the architecture for a police state in the US, it has created the largest set of mass surveillance programs in the history of the world, while covertlyweakening Internet security and privacy for everyone on the planet. Without privacy and robust data protections under the law, no real individual citizen sovereignty within a state and society is possible.

NSA is doing this deliberately, systematically, and in secret. Even if we take NSA at its word—it's intention to only target persons suspected of terrorism as it relates to foreign intelligence— they're clearly now collecting and storing as much of our communications as possible.

NSA has inverted the heart of the democratic paradigm in which the government acts in public and our personal lives are private. Now everyone's personal and private lives and associated transaction and data history becomes the equivalent of secret government property, held for years as pre-crime data just in case it is needed in the future – secret dossiers of the State - while attempts to expose the government are met with the heavy hand of criminal prosecution.

The words of US Senator Frank Church during the hearings he conducted on the abuses of national security power in the 1970s are worthy of reminding us what can happen when a state sponsored surveillance regime is used as the excuse to keep us safe at the expense of liberty and freedom.

"If a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of government to know. Such is the capacity of technology."

People in America and around the world should not have to worry about protecting themselves from an unhinged United States government, unchained from its own Constitution, but worry they must. And the government should not, under the guise of protecting its own citizenry, conduct mass dragnet surveillancein secret, let alone of the entire world while publicly crushing anyone who tries to expose it.

I respectfully suggest that your Committee duly examine the critical need for transparency and legal accountability to enforce fundamental and vitally precious citizen rights to speech and association while protecting those who exposegovernment malfeasance and wrongdoing as well as providing for robustprotections against unwarranted "search and seizure" by any foreign power, state surveillance agency or corporate entity.

I hope that your Committee will consider a European Union-wide law that all EU-to EU Internet links and nodes must be encrypted, with open source encryption technology made available for the widest possible use wherever practical, while also audited by the EU.

What we see now revealed on a global scale creates the power of mass- surveillance and eludes effective control by current data and privacy protection regulations.

How do your member states protect themselves from the predations of the surveillance regime?

There is a distinct need for policies that prohibit third party countries and commercial concerns from accessing and compromising personal data, while also covering vendors and suppliers of IT systems and products.

There is also the need to put in place the power to prosecute and hold accountable those transnational companies and entities from secretly compromising the very infrastructure that society depends on for business and trade – even considering the need for a comprehensive data protection treaty between member states and the US.

'Prism-proofing' your member state Internet hosting and service providers is now critical given how data is not so much broken into as it is taken and renditioned by the surveillance state.

It is the constant possibility of the unequal gaze and reality of surveillance and observation (real or imagined) that stultifies society, renders creativity mute, and erodes our freedom with the acid served up by the potent brew of secrecy and surveillance for the sake of security while forsaking our liberties as the price we must pay. I fundamentally reject this dystopian premise and promise given what happened to me.

I was fortunate that I did not end up in an actual prison (having lived the virtual version for a number of years) for coming out of the system and speaking truth to and of power - a dangerous act of civil disobedience and individuality for sure in these times - expressing one's fundamental and inalienable right to individual sovereignty in the face of a government bent on destroying it.

The last thing a free and open society needs is a digital fence around us - with the barbed wire of surveillance not only keeping track of our comings and goings, yet now increasingly wanting to know what we think and feel - the very essence of who we are and share as human beings.

Thank you.
========