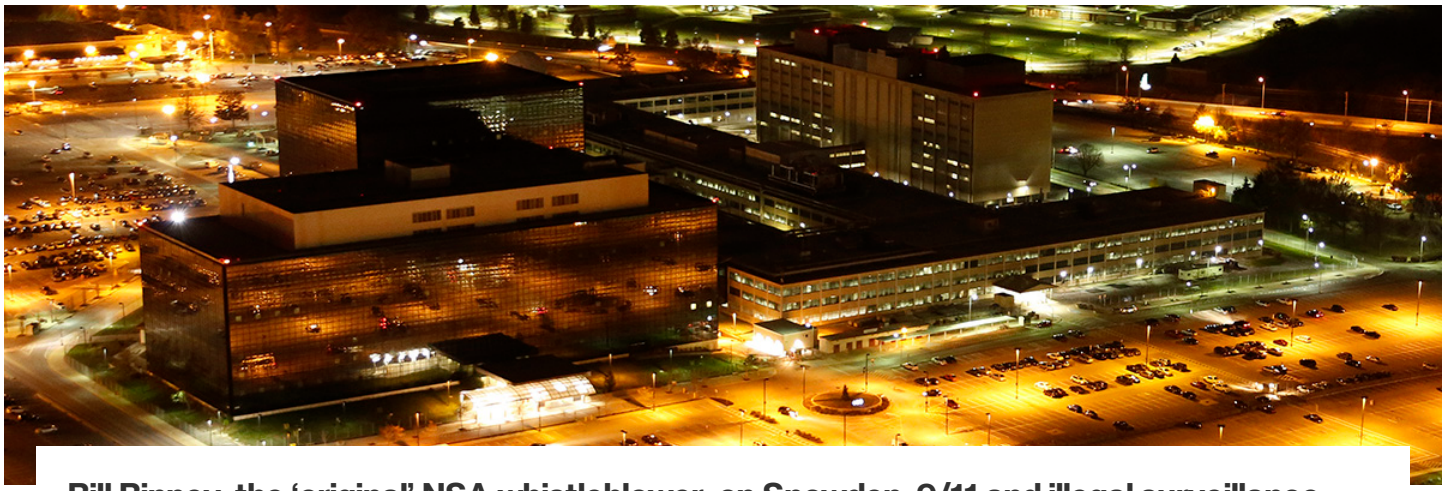
TREVOR PAGLEN



Bill Binney, the 'original' NSA whistleblower, on Snowden, 9/11 and illegal surveillance

2

Fiona O'Cleirigh

Always a patriot: Computer Weekly talks to Bill Binney, the senior NSA official who blew the whistle before Edward Snowden

He started his career as a patriot and ended it as a patriot – and he thinks Ed Snowden is a patriot as well. Computer Weekly talks to Bill Binney, the senior NSA official who blew the whistle before Snowden.

Bill Binney believes that 9/11 was preventable. A month after it happened, he resigned in protest from the US National Security Agency (NSA).

Binney was part of an elite NSA team which designed and built an intelligence-gathering system to target and collect data on terrorism threats.

He belongs to an intimate group of four whistleblowers, each of whom left the NSA after raising concerns about failures in the agency's intelligence-gathering capabilities.

Binney's track record is impeccable. He spent four years in the Army Security Agency during the Vietnam War before transferring to the NSA in 1970.

He rose to become technical director of World Geopolitical & Military Analysis at the Signals Intelligence Automation Research Center (SARC), a 6,000-strong research centre he co-founded at NSA's headquarters in Maryland, US.

In a wide-ranging interview with Computer Weekly, Binney raises serious concerns over the NSA's current surveillance programmes.

He alleges:

- The NSA buried key intelligence that could have prevented 9/11;
- The agency's bulk data collection from internet and telephone communications is unconstitutional and illegal in the US;
- The NSA is ineffective at preventing terrorism because analysts are too swamped with information under its bulk collection programme;
- Electronic intelligence gathering is being used for covert law enforcement, political control and industrial espionage, both in and beyond the US;
- Edward Snowden's leaks could have been prevented.

Binney's story

As Binney tells it, the NSA made significant breakthroughs in intelligence gathering in 1998, when its engineers worked out how to re-assemble diverse packets of data gathered from fibre optic cables.

The process, known as sessionising, could allow the NSA to reconstruct communication records from a trail of data passing through the cables.

Binney worked at SARC, together with fellow whistleblower Ed Loomis and a small team of specialists, to build technology to harvest data from fibre optic cables. The result was Thinthread, an in-house process "for collection and rapid analysis of billions of electronic records".

SARC chief Loomis and Binney divided the workload between them. While Loomis focused on the front end, Binney concentrated on analysing and managing the data.

Targeting data

Binney was responsible for feeding targeting rules gleaned from the analysis back into the analytical tools. This self-refinement was key, allowing analysts to hone in on their targets, without the need for mass data collection.

Features of Thinthread

- Graphed metadata to locate targets of interest
- Analysis refined rules for future data acquisition
- Less storage needed than with unfiltered bulk collection
- Encryption used to protect data subjects until targeted
- Legal and constitutional

"Once you analyse the data, you know what you want and you feed those rules back in to the front end that acquires data, and that then drives the acquisition of information," he says.

Binney had planned to automate the feedback process, but the NSA cancelled the project before the work could be completed. "I never got to it, fortunately, so the NSA doesn't have it now," he says.

Metadata is key to NSA surveillance

Metadata was key to Thinthread then and key to the NSA now. By using this "data about data", the NSA can tag and categorise communications, allowing analysts to see very quickly the communities that are interacting on the network as they do it.

Trying to correlate the raw data itself would have proved cumbersome. "But you do it from metadata," says Binney, "you see the groupings and interactions and you can see how you could pull those groupings together and then pull the content out and see what their activity is."

Protecting privacy

Crucially, Thinthread used automatic encryption to protect the identities of US citizens, a requirement of the Foreign Intelligence Surveillance Act and the Fourth Amendment of the US constitution.

The data could only have been decrypted if a judge found probable cause to believe the target was connected with serious crime, including terrorism.

Data belonging to non-US citizens was also protected, unless it could be shown they were relevant to the investigation underway, says Binney.

"For everybody who came in who was not in the zone of suspicion – or even those who were in the zone of suspicion, if they were Americans – we would certainly encrypt all the data till you could show that they were a part of that activity. If you could show that, then you would un-encrypt them and then target them," he says.

"It was a very disciplined, legal, constitutionally acceptable process."

The Bumblehive

Because the technology allowed targeted surveillance, it did not require the NSA to build vast repositories to store data.

That made the complete programme a lot cheaper than the NSA's Utah Data Center – code-named Bumblehive – in Bluffdale.

The mammoth "mission data repository" has cost at least $1.5bn and was designed specifically to store digital data gleaned from the internet.

Reconstructing evidence

One of NSA whistleblower Bill Binney's main concerns is how the NSA uses the data it gathers, not just in the US but also

internationally.

Concerns were raised last year, when a report in Reuters revealed that the US Drug Enforcement Agency (DEA) was using NSA phone intercepts, alongside domestic wiretaps and informants, to build up a database on drug-related crime.

Documents seen by the news agency showed that law enforcement agents had been directed to conceal how such investigations begin – from defense lawyers and sometimes from prosecutors and judges.

Because illegally obtained evidence is not admissible in court, the DEA altered and recreated its investigative trail in a process known as "parallel construction".

This was then substituted for the NSA data as evidence in the courts.

Life incarceration

New US legislation – the National Defense Authorization Act section 1021 – has enabled the president to declare a suspect a terrorist threat, with indefinite military detention without trial.

Binney believes that the ability to reconstruct evidence from illegal NSA surveillance may ultimately lead to life incarceration without due process for American citizens.

It is a denial of due process, in that it prevents effective challenges by lawyers, Binney claims. "I call that perjury. It is a planned, programmed perjury policy run by the Department of Justice of the United States. It's run worldwide. It's not limited to the US."

Its Cray XC30 supercomputer can handle workloads exceeding 100 petaflops and is expected to be the first facility that can acquire and store a yottabyte of data.

"You didn't need all that storage," Binney explains, "because you were focused on targets of interest and zones of suspicion around them, based on graphing techniques, social networking and other criteria."

Thinthread cancelled

The Thinthread project, which required an estimated $300m in funding, was never taken up as promoted by its developers. After several years of work, Binney and Loomis were told of its cancellation three weeks before 9/11.

Instead, the NSA chose a programme run by contractors called Trailblazer. The agency spent billions, but never progressed beyond the prototype.

The project that ultimately took hold was Stellarwind, which Binney claims is "a bastardised version of Thinthread".

"It was subverted, to get rid of the encryption, and the NSA decided to get rid of the filtering upfront. Instead of targeting, it went for everything."

Analysts 'swamped with data'

With Stellarwind and its successor projects, Binney argues that the NSA has turned a large proportion of the world's population into data subjects. The upshot is a burgeoning mass of data that swamps the agency's analysts.

"That's the problem," says Binney. "With this bulk acquisition of data on everybody, they've inundated their analysts with data. Unless they do a very focused attack, they're buried in information, and that's why they can't succeed."

9/11 intelligence missed

It later emerged that the NSA may have overlooked key intelligence that might have prevented the 9/11 terrorists attacks.

After Binney and Loomis's departure, Thomas Drake, who worked for the NSA's Defense Intelligence Senior Executive Service, tried to get authorisation for Thinthread to go operational.

He failed, but he did obtain funding to use Thinthread for a content evaluation of NSA databases.

The exercise revealed that the NSA had intelligence about Al Qaeda hijackers before and after 9/11 but had not shared it with the FBI or other government agencies. An early 2001 report on Al Qaeda's movements had also been suppressed.

"Make no mistake. That data and the analytic report could have – should have – prevented 9/11. Top NSA management knew that. They knew that I knew that," Drake later wrote in an open memorandum to President Obama.

The project was immediately shut down, Drake claims: "In spring 2002, the remnants of Thinthread were unceremoniously put on the shelf in NSA's 'Indiana Jones' data warehouse, never to be seen again."

NSA surveillance 'is unconstitutional'

The NSA's surveillance programme as it exists today, Binney insists, is unconstitutional in the US.

One area of concern is the NSA's surveillance of US and foreign citizens, through a programme known as Fairview.

ELECTROSPACES

Fairview fibre optic taps

Whereas Prism targets data already processed by social media companies, Fairview taps data directly from the fibre optic telephone cables, with no filtering. "They put their devices on the line and take the entire line. Everything," says Binney.

Fairview gives the NSA access to data from foreign telecoms companies via an unnamed US telecoms intermediary. The programme is also the main data acquisition system for inside America, says Binney.

Slides leaked by former NSA contractor Edward Snowden showed about 80 to 100 fibre optic taps inside the continental US. Each would have cost tens of millions of dollars, if not hundreds, to build, says Binney.

"Most of them were not along the coast, which meant that they weren't targeting the transoceanic cables where they come up and surface on the coast. They were targeting inside."

Strangers on the line

The NSA's line-tapping facility at an AT&T facility in San Francisco was exposed by an AT&T technician turned whistleblower, Mark Klein, back in 2007.

Calls to bring NSA into line with US law

Binney and his fellow whistleblowers have made an open appeal to President Obama, with a list of 21 recommendations to bring the NSA's work in line with US law.

In another document – *NSA insiders reveal what went wrong* – they draw the president's attention to the finding of Obama's own Review Group on NSA efficacy: "Exactly zero terrorist plots have been prevented by NSA's bulk trawling for telephone call records."

The NSA had transferred the fibre lines to a secret room where analysts could take the data right off the fibre line using equipment known as Narus devices, which were capable of reconstructing all the packet communications along the fibre lines at the rate of 10Gbps.

One device, Binney reckons, could manage over 100 billion 1,000-character emails, every day. "And they have 80 to 100 different sites, so multiply that up and you can get an idea of the magnitude of data that they can collect."

Questions have been raised about the legality of the NSA's surveillance operations overseas. But Binney doubts that the NSA ever considered the legal implications outside the US.

"They were [more] concerned about how to cover up their activity from Congress and the courts here in the US because we have laws against them doing this kind of activity."

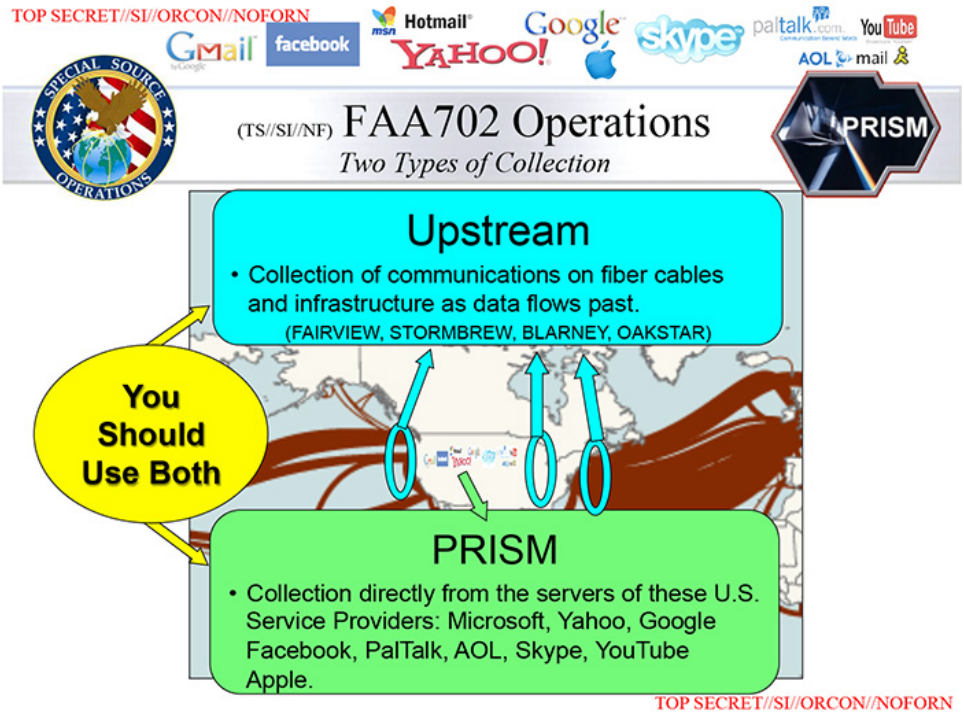
Over 'two billion people affected by NSA surveillance'

Overall, Binney suspects that somewhere between two and three billion people are affected by NSA surveillance worldwide.

"This is not restricted to the internet dealing with computer-to-computer, peer-type communications. It is also dealing with the public switch telephone network. So it is getting everybody on both systems," he says.

Bulk data collection 'illegal'

The Fourth Amendment of the American Constitution upholds the right to privacy and the freedom from unwarranted intrusion for US citizens.



Collection methods: The NSA collects traffic in two ways – by tapping into fiber optic cables (upstream collection) and directly from US service providers (Prism)

Binney claims the NSA's surveillance activities are a clear violation of the Constitution.

The NSA's officials are in violation of their oath of office, to protect and defend the Constitution, he says. "What they were doing here was an impeachable activity."

Such unconstitutional behaviour is, ultimately, pointless, claim Binney and his fellow whistleblowers, who have written an open memorandum to the president.

In it, they cite the finding of Obama's own Review Group on NSA efficacy: "Exactly zero terrorist plots have been prevented by NSA's bulk trawling for telephone call records."

NSA response

Computer Weekly asked the NSA to address key allegations made by Bill Binney, specifically regarding suppressed information around 9/11 and the use of unconstitutional measures to collect data on US citizens.

An NSA spokesperson responded with the following statement:

"In carrying out its mission, NSA collects only what it is authorised by law to collect for valid foreign intelligence purposes.

The communications of people who are not foreign intelligence targets are of no use to the agency.

"In January, President Obama issued US Presidential Policy Directive 28, which affirms that all persons – regardless of nationality – have legitimate privacy interests in the handling of their personal information, and that privacy and civil liberties shall be integral considerations in the planning of US signals intelligence activities.

"All of NSA's operations are conducted in strict accordance with the rule of law, including the president's new directive."

Political blackmail

There are fears, for example, that data the NSA collects from the internet could be used to blackmail or compromise people who do not support the US government's policies.

"This is J. Edgar Hoover on supersteroids, not just in the US but worldwide. So, yeah, they can do anything they want," he says.

Binney suggests that NSA data is already being used as a tool of political interference. "They've been using it against the Tea Party, the Occupy groups, even religious organisations trying to get politically active."

He says the NSA has specifically been working through the Internal Revenue Service (IRS). "That's being used to stop organisations that want to become politically active, as well as socially active, from getting 501(c)(3) status – which means tax-exempt status over here."

Contractor abuse

Contractors have access to NSA data, and may be less scrupulous about how they use that information than government employees.

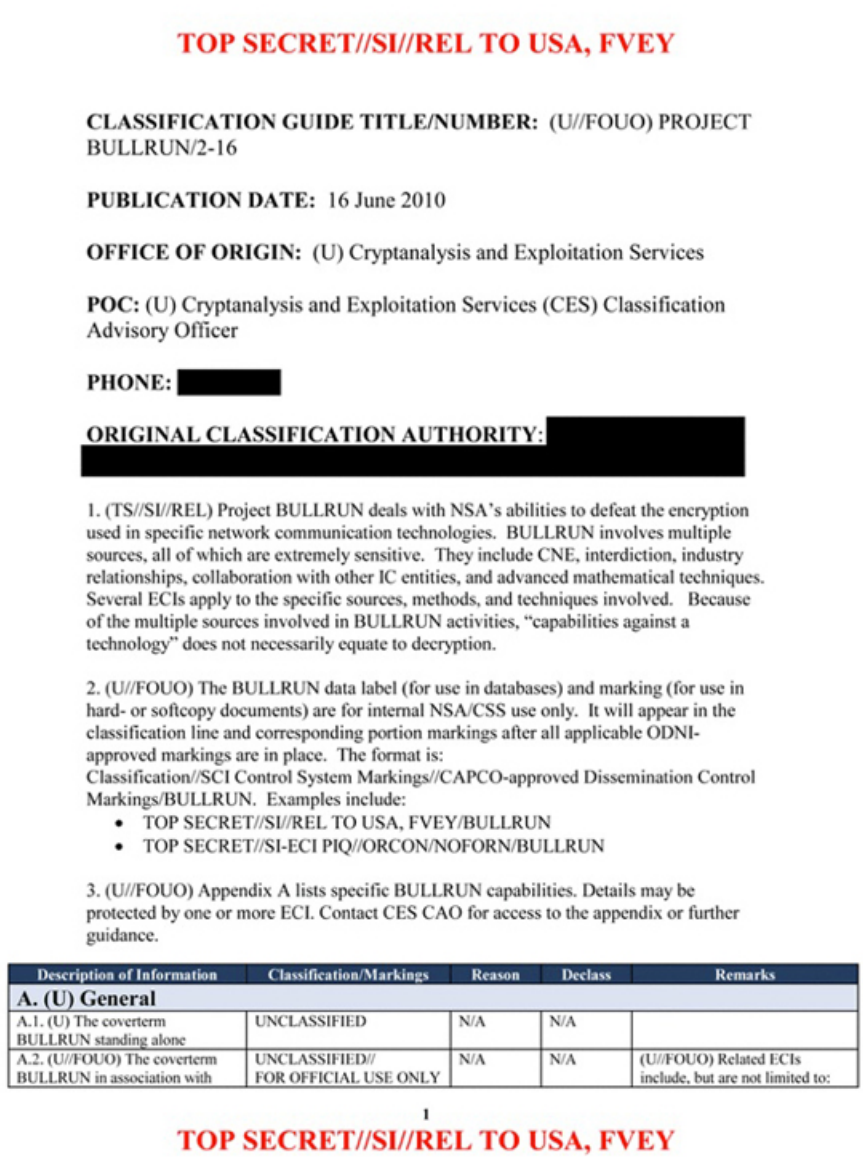
"When they want to do industrial espionage, they have access to the information that could produce that kind of result," says Binney.

In fact, documents released by Snowden show NSA had been spying on Brazilian oil company Petrobras, taking intelligence gathering far beyond its national security remit.

"The potential there is to be worldwide with this kind of activity," says Binney.

NSA policies increase risk of hacking by foreign governments

He is concerned too that the NSA's activities are exposing the US to foreign states' electronic intelligence gathering.



TOP SECRET//SI//REL TO USA, FVEY

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

2. (U//FOUO) The BULLRUN data label (for use in databases) and marking (for use in hard- or softcopy documents) are for internal NSA/CSS use only. It will appear in the classification line and corresponding portion markings after all applicable ODNI-approved markings are in place. The format is:
Classification//SCI Control System Markings//CAPCO-approved Dissemination Control Markings/BULLRUN. Examples include:
- TOP SECRET//SI//REL TO USA, FVEY/BULLRUN
- TOP SECRET//SI-ECI PIQ//ORCON/NOFORN/BULLRUN

3. (U//FOUO) Appendix A lists specific BULLRUN capabilities. Details may be protected by one or more ECI. Contact CES CAO for access to the appendix or further guidance.

Description of Information	Classification/Markings	Reason	Declass	Remarks
A. (U) General				
A.1. (U) The coverterm BULLRUN standing alone	UNCLASSIFIED	N/A	N/A	
A.2. (U//FOUO) The coverterm BULLRUN in association with	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	(U//FOUO) Related ECIs include, but are not limited to:

1

TOP SECRET//SI//REL TO USA, FVEY

Bullrun: leaked NSA document shows how the agency is defeating encryption technology.

He is highly critical of Bullrun, a programme that was designed – according to the NSA's own leaked documents (*see image left*) – "to defeat the encryption used in specific network communication technologies".

Binney believes this is finite thinking. "NSA's not the only one smart enough to get through these things, find them and use them. Other governments can do it, other hackers can do it. So they are basically opening up the networks."

Asked if he would ever consider going back to the NSA to pick up a Fourth Amendment-compliant version of the project if asked, Binney said no, although the data-targeting problem, he feels, is fixable.

"I would never do the automation for them because they can't be trusted. I mean, what they've done so far, they've had no reservation in violating our constitution and the constitutional rights of every citizen in the US, let alone everybody around the world. You cannot trust any organisation that does that. You can't."

Snowden leaks could have been prevented

Ironically, under Thinthread, whistleblowing would have been much harder. Binney's programme had proposed a system of internal NSA monitoring, but he claims it was opposed by analysts, who resented excessive supervision.

Management were also against it, as they did not want it known how they were spending money and shifting money around between programmes and what kind of return they were getting, says Binney.

"If it became known," he says, "and Congress found out about it, they could cancel programmes that were not

efficient and it would destroy empires that were being built internally in the NSA."

Under Thinthread, Snowden's mass downloads would have been impossible, he claims. "If we had that program running when he started downloading something, why, we'd have known it as soon as he started doing it."

Patriot or traitor?

In the debate on Snowden as either patriot or traitor, Binney opts for the former: "I would put him as a patriot, yes. He is trying to stand up for the Constitution. That's what we all did and our government attacked us for doing that. So, in my view, the government is the criminal here."

While members of the public have thanked Binney in person for speaking out against what he saw as abuse of the Constitution, the NSA's attitude to the whistleblowers was less welcoming.

"When we went into the private consulting business, every contract we ever got was cancelled by either the FBI or NSA," claims Binney.

"They had us under threat of indictment, for a number of years," he says. "We were basically untouchable as a commodity. They simply blackballed us in terms of employment totally."

Binney suggests that current NSA technical developers – who might prefer a different way of collecting data – feel threatened and dare not challenge the status quo.

"Right now, internal security has a programme that's like the Stasi, with people in the same business working with one another, watching each other and reporting back," he says.

Public opinion in US shifting towards Snowden

Yet public opinion in America is shifting in favour of Snowden and away from the government. An opinion poll commissioned by Tresorit, a cloud storage service, showed that 55% "believed he did the right thing". Of those, 80% felt he had exposed constitutional violations.

Last June, two representatives in Congress – a young libertarian Republican and a veteran civil rights Democrat – proposed bipartisan legislation to defund the NSA's phone record collection programme. The bill failed by 217 votes to 205.

"And the reason they did it," says Binney, "was they found they weren't being told the truth by the intelligence committees inside Congress. So Congress is lying to [itself] about what's going on."

Worried about the future

Binney worries for the future. America, he believes, is turning away from democratic governance. "This is what happens in totalitarian states. They slowly evolve. We're frogs in the water and they're heating the water ever so slowly. Eventually, they'll get us cooked, as they raise the level and we don't jump out.

"As long as they do it slowly," he insists, "we won't jump out."

William Binney - The man behind the leak

William Edward Binney was born and raised in central western Pennsylvania. With a degree in mathematics, he volunteered to join the US army in Europe in 1965 – working at the Army Security Agency in Germany, which held command of all US signal intelligence units in Europe.

Considered suitable for training as an analyst, Binney spent four years with the military before transferring to the NSA, the US electronic communications monitoring agency, achieving 37 years combined service in both. His work focused on data traffic analysis, data systems analysis and code-breaking.

In 1997, Binney became the technical director of World Geopolitical & Military Analysis at the Signals Intelligence Automation Research Center (SARC), a 6,000-strong operations unit which he co-founded.

He worked with a small team to develop Thinthread, a programme for the automated, targeted upstream acquisition of security data from fibre optic lines.

He retired from the NSA in October 2001, appalled by the agency's failure to prevent 9/11.

He became part of an intimate group of four NSA whistleblowers. They included Ed Loomis and Kirk Wiebe, senior officials at SARC who worked alongside Binney, and Thomas Drake, who was part of the NSA's Defense Intelligence Senior Executive Service. Between them they had chalked up 144 years experience in the NSA.

Binney's home was raided by the FBI in 2007 at gunpoint, following public criticism of his former employer.

This was last published in April 2015

Read more on Business process management (BPM)

ALL NEWS IN DEPTH BLOG POSTS OPINION

Bazinga! Bizagi! -- BPM tools for digital transformation

Large global companies still manage supply chain with phone, fax and email

Combine data mining and simulation to maximise process improvement

HR analytics tools promise edge in war for talent

Load More

Join the conversation

2 comments

Share your comment

Send me notifications when other members comment.

Add My Comment

Oldest ▼

[-] ncberns

- 5 Jun 2016 8:32 AM

We demand to know the Truth. Then arrest and vilify the Truth Sayers because we're so afraid of the Truth. Governments pass laws making whistle blowing illegal, Even the recording of illegal activity has been made a crime.

We have to decide if Big Business and other evil-doers should be protected from any responsibility for their actions. Or we want to be guided by truth and transparency.

One is about control. The other is about freedom. Can't have both.

Reply

[-] AlbertGareev

- 23 Aug 2016 11:16 AM

Unfortunately, there's no single absolute truth. Government agencies may do what they assume is "right", and that includes Guantanamo. Terrorists also somehow believe that they're actions are justified. How to break this cycle?..

Reply

SearchCIO

2016 mergers and acquisitions in tech: Our top 5 picks

We look back at the torrid pace of 2016 mergers and acquisitions in tech. Here are the top five deals and a post-mortem on last ...

IT conferences 2016: The year in photos

In this IT conferences 2016 Instagram roundup, take a look back at some of the best moments from our recent travels.