Edward Snowden NSA files: secret surveillance and our revelations so far

NSA headquarters in Fort Meade, Maryland. Photograph: Patrick Semansky/AP

In the 11 weeks since the Guardian published its first revelations from top-secret material leaked by the NSA contractor Edward Snowden, the paper has published more than 300 stories on the surveillance state and the political fallout from the revelations.

The disclosures shed unprecedented light on the scale and sophistication of surveillance on both sides of the Atlantic – and the secret laws underpinning such programmes. As publication continued, the UK government brought substantial pressure to bear, leading to the Guardian's decision to destroy a copy of the GCHQ documents: those stored in its London offices.

Reporting based on caches of internal documents from both the NSA and GCHQ continues from New York and Rio de Janeiro, but the key revelations to date are below.

NSA

The first revelation of the NSA files was the publication of a top-secret court order against Verizon Business Services, mandating it to hand over the call records – numbers called, when calls took place, and for how long – for all of its customers.

Subsequent reporting confirmed similar orders, made under Section 215 of the Patriot Act, existed for the other telecoms firms operating in the US, and were used to maintain a database of all call records – a continuation of the warrantless wiretapping systems begun under George Bush.

Other stories centred on programmes that allowed for large-scale collection of people's data without any individual warrants. The first – and best known – is Prism, a system allowing the NSA easy access to the personal information of non-US persons from the databases of some of the world's biggest tech companies, including Apple, Google, Microsoft and Yahoo. Later, it emerged Microsoft had worked to circumvent its own encryption to enable NSA access to customer records.

Other data is collected from extensive cable tapping operations: the collection of both metadata and the content of communications travelling through the fibre-optic cables that make up the backbone of the internet.

The NSA's collection operation – collectively referred to as the "Upstream" programme – relies on co-operation with four US telecoms providers. The identity of each is a tightly guarded secret of the agency, with each referred by the codenames STROMBREW, FAIRVIEW, BLARNEY and OAKSTAR. To date, the firms behind each have not been unmasked.

Details of the system, known as XKeyscore, used to collect, process and search these vast troves of data were also uncovered. One presentation, published in redacted form in the Guardian, claimed the system allowed NSA analysts to query "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata. The system works almost in real-time, documents claimed.

But just as important as the technical capabilities of the NSA are the legal and policy safeguards restricting their actions. As the first NSA files stories were published, senior Obama administration officials – and the president himself – gave repeated reassurances that Americans' privacy (if not that of foreigners) was strictly protected.

Secret documents presented a very different picture. Targeting policies dating from 2009 – the rules on what the agency can target and which data they are allowed to keep – show the large range of circumstances in which the agency could retain data on US citizens, if it had been "inadvertently" swept up in its mass-collection systems.

US data that couldn't be separated from foreign data due to technical limitations could be kept until it was examined, the documents ruled. Once examined, it could be kept if it contained usable intelligence, information on criminal activity, threat of harm to people or property, was encrypted, or was believed to contain any information relevant to cybersecurity. Under certain circumstances, even attorney-client conversation could be retained.

The rules were relaxed still further two years later, further documents revealed, allowing analysts to search for US citizens within their warrantless databases, under certain circumstances.

GCHQ

The first reporting on GCHQ centred on the UK intelligence agency's access to the Prism, which had been used to generate 197 intelligence reports for the UK in a year. Those first reports prompted the foreign secretary, William Hague, in June to reassure parliament that UK intelligence agencies work within "the strongest systems of checks and balances for secret intelligence anywhere in the world".

That's not what GCHQ analysts were telling their NSA counterparts in confidential briefings. One, setting out the legal framework in the UK that allows for the lawful interception of communications in and out of the UK (including internet cables entering and exiting the country), without individual warrants was stark.

The senior GCHQ legal adviser noted to his NSA counterparts that "[w]e have a light oversight regime compared with the US", adding that the parliamentary committee meant to oversee the agency had "always been exceptionally good at understanding the need to keep our work secret".

This apparently light regime has allowed GCHQ to set up a surveillance operation that its analysts believe is on a larger scale than anything the NSA directly operates: the Tempora programme. Tempora allows GCHQ to harvest hundreds of gigabytes of data entering and leaving the UK each second, storing content for three days and metadata for up to 30. The collected information includes websites visited, emails sent and received, instant messages, calls, passwords and more – and the agency has individual tools centred on searching through each.

The programme, like its smaller-scale US equivalent, centres on probes placed on fibre-optic cables of some of the world's biggest telecoms giants. GCHQ has probes on the vast majority of internet cables coming into and out of the country, but can only collect from about a fifth of these at any one time.

The telecoms firms involved in Tempora were later named, initially in the German press, as BT, Verizon Business, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute. Details on the nature of the relationship between the firms and the agency have not emerged to date, but those who responded to requests for comments stressed their obligation to comply with the laws of the countries in which they operate. The telecoms providers are now facing possible legal action over their involvement with the program.

By May 2012, 300 GCHQ analysts and 250 NSA analysts had direct access to search this data at will.

The Tempora co-operation serves as one example of an increasingly close relationship. The latest Guardian story on GCHQ – published more than a week after the destruction of computer equipment in the basement of the newspaper's offices in King's Place – showed the NSA was providing millions of pounds of funding each year to GCHQ.

The documents also showed the NSA expects results from GCHQ in return for its cash. One, dating from 2010 "raised a number of issues with regards to meeting NSA's minimum expectations". It said GCHQ "still remains short of the full NSA ask". Another strategy briefing remarked: "GCHQ must pull its weight and be seen to pull its weight."