THE IRISH TIMES

Dataspying: Does it work?

Revelations about the US National Security Agency's vast Prism surveillance programme highlight privacy and security issues. Is there any benefit to it?

By: Davin O'Dwyer – June 15, 2013

In the late 18th century the English philosopher Jeremy Bentham conceived of a prison from which the watchman could secretly monitor the inmates. It was a large cylindrical building many stories high, with a tall control tower in the centre and the cells arrayed around the perimeter. The knowledge that they might be watched at any time would be enough, Bentham believed, to ensure obedience. He called his vision the Panopticon.

Before leaking his trove of data last week about the US National Security Agency's vast surveillance programme, Edward Snowden invoked Bentham's creation in a correspondence with the investigative journalist Barton Gellman. "In one step, we've managed to justify the operation of the Panopticon," Snowden wrote.

The parallel was clear to Snowden: the NSA is in the process of building an apparatus that can watch anybody who communicates digitally. And it is a process so cloaked in secrecy that most people will never realise they are under surveillance.

What does a modern-day Panopticon look like? Instead of a cylindrical building, picture a sprawling complex in the Utah desert. It is here in Bluffdale, in the shadow of the Oquirrh Mountains, that the NSA is constructing a $2 billion maximum-security data centre.

According to the security expert James Bamford, writing in Wired, the centre is capable of storing a yottabyte of data, an almost unimaginably vast amount of information. ("Yotta" denotes a 1 followed by 24 zeros.)

There has been considerable speculation about how, exactly, the Prism programme that Snowden revealed provides the NSA with access to data from Google, Facebook, Appleand other technology firms, but it is clear the NSA is preparing for a future when it has access to an unprecedented amount of data.

Bluffdale might not look like Bentham's Panopticon, but Snowden's analogy is apt. One former senior NSA official, William Binney, is under no illusions about where we are heading. Interviewed by Bamford, he held his thumb and forefinger close together and said, "We are, like, that far from a turnkey totalitarian state."

The revelations bring into stark relief many of the privacy and security issues we have been awkwardly avoiding for a decade or more. Are these intrusions a reasonable price to pay for US security? Will the age of digital global communications inevitably lead to surveillance states? Can traditional notions of privacy survive these upheavals?

These are big questions with no easy answers. It's no wonder so many pundits are happier debating whether Snowden is a hero or a traitor.

Civil liberties

"It's not useful to discuss whether you would rather be blown up by a terrorist or have the NSA access my phone records," says Julian Sanchez, a research fellow at the Cato Institute in Washington who writes on civil liberties and privacy issues.

"Between 1970 and 2007 the risk of dying in a terrorist attack was one in 35 million. That's not to trivialise it, but in the grand scheme the risk isn't appropriate to the costs or invasions of privacy we're seeing. The question is not just do we want to fight terrorism; it is whether the indiscriminate acquisition of phone records will bring us a reduction in the risk of terror deaths, compared to more narrowly getting that information."

From the perspective of a cost-benefit analysis, then, NSA programmes such as Prism and Boundless Informant are debatable, but Sanchez also questions their efficacy. "You look at the track record of claims for these programmes and they are not good. The original wiretapping by the Bush administration was introduced in the wake of 9/11 – supposedly no time to be squeamish about civil liberties – and a few years later the intelligence agencies admitted in the Unclassified Report on the President's Surveillance Programme, from 2009, that the wiretapping was of no greater value than other tools they used. It was difficult to point to examples where it made a big difference. What is clear is that it wasted resources and time of investigators."

The most indefatigable defender of online civil rights and the fourth amendment of the US constitution in recent years has been the Electronic Frontier Foundation, a San Francisco-based activist group. Snowden has a foundation sticker on his laptop, a none too subtle hint at his sympathies.

"Aspects of these revelations are just shedding further light on things we suspected were occurring," says Peter Eckersley, the foundation's technology-projects director. "But there is still a lot we don't know about the scale and scope of those revelations. I don't think people are prepared for the kind of power transformations that this will bring. It's technology that can turn incredibly nasty incredibly quickly if you have a government that harbours malign intentions towards its citizens."

Does he see how the situation can be improved? "I think there are two ways you can jam the genie back in the bottle, and both are hard. One is about seriously building technical preventions

against this surveillance, but we need to be aware that the engineering challenges are kind of daunting.

“The other road we can go down is building better legal protections – what I call verifiable oversight. There is some oversight, but the mechanisms have clearly been inadequate for the incredible amount of power that the NSA is wielding here.”

That inadequate oversight has repercussions beyond mere fourth-amendment violations; it is likely to transform our notions of privacy in the age of cloud computing, status updates and geolocatable smartphones. One of the leading scholars of online privacy, Prof Helen Nissenbaum of New York University, sees these revelations as particularly challenging. “My theory suggests that we have certain expectations of privacy, of how information flows in society, and what I’ve argued is that they are very much keyed to particular contexts and particular functions,” she says. “So I may have certain expectations with regard to various government actors and completely different expectations with regard to other actors.”

Nissenbaum points out that the NSA’s purpose – defending against security threats – “does carry positive moral weight” but that the method risks “radically altering our sense of this medium”.

“I grew up in South Africa, and you would not talk freely on the phone,” she says. “When I moved to the States it took me a long time to decide I could speak my mind on the phone. You always have this sense, not that I was doing anything important enough, but you always had that sense that someone could be listening to this phone call. It’s not freedom.”

Abuse of power

How do we prevent the rise of misplaced power? Julian Sanchez is optimistic that US democracy is strong enough to prevent the country slipping into a total abuse of power. “It’s inevitable only if we decide it’s inevitable. A surveillance state is not the inexorable truth,” he says. “We make these choices, we decide if that can happen, but whether they build that infrastructure, whether they construct the universal surveillance machine . . . that is not inevitable.”

Perhaps, but that complex in Utah and the vast apparatus that feeds it with data is on its way. When the great Irish conservative philosopher Edmund Burke saw Bentham’s plans for the Panopticon, with the central tower offering not just a covert view but also immense power, he reputedly said: “There’s the spider in the web!”

We’re in the web already, but it’s not too late to determine what sort of spider will keep us company.