Opinion: After Paris, it's traditional detective work that will keep us safe, not mass surveillance

November 20 2015, by Pete Fussey

Credit: AI-generated image (disclaimer)

Before the dust has even settled from the attacks on Paris, familiar calls for greater surveillance powers are surfacing. The desire for greater security is understandable, but that doesn't mean we should suspend our judgement on the measures proposed to bring it about.

In the aftermath of the attack, prime minister David Cameron intimated a desire to accelerate the passage of the Investigatory Powers bill through parliament, while in the US, CIA chief John Brennan called for greater powers for the intelligence and security services. Such sentiments reflect a longstanding attitude championing the benefits of technological solutions.

The rush to legislate and grant sweeping powers has led to untried and untested provisions and incoherent laws that complicate security practice. Following the Charlie Hebdo attacks in January 2015 the French government enacted new surveillance laws that introduced warrantless searches, the requirement for ISPs to collect communications metadata, and watered-down oversight regimes. In the UK, the response to the September 11 attacks included rushing through powers in the Anti-Terrorism Crime and Security Act 2001, but it's the more considered Terrorism Act 2000 and other laws already on the books that have proved more useful when it comes to convicting terrorists.

Politicians make claims about the number of threats and plots averted by the secret services' use of surveillance data. But this rhetoric is rarely backed up with facts, and masks the practical and ethical problems that strong powers of mass surveillance bring.

A technocratic mirage

Those supporting mass surveillance of digital communications data have to conclusively demonstrate its usefulness. The history of technocratic approaches to security is littered with claims of effectiveness that are overstated, unproven or just wrong. Such claims must be treated with scepticism, not least because money spent here will divert scarce resources away from traditional intelligence and policing techniques that are tried and tested.

As a journalist and confident of Edward Snowden, Glenn Greenwald said: "Every terrorist who's capable of tying their own shoes has long known that the US and UK government are trying to monitor their communications in every way that they can." Academic research has consistently shown terrorists are innovative in their use of technology in order to evade detection. A Flashpoint intelligence report in 2014 revealed that there had been no expansion of terrorists' use of encryption technology following Snowden's revelations, largely because those that could were already using it.

Following the Snowden revelations president Obama established a review into their use which concluded:

The information contributed to terrorist investigations by the use of section 215 [of the PATRIOT Act] telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional … orders.

Traditional methods have, even during the internet era, consistently prevented and disrupted terrorist attacks. For every anecdote supporting the usefulness of online surveillance, others exist to underline the role of more mundane interventions and police detective work. Shoe-bomber Richard Reid's attempt to bring down an airliner, the attempt to bomb Times Square in 2010, and this year's Thalys train attack at Pas-de-Calais were all averted by the actions of observant and brave members of the public.

The best intelligence is human

It's widely accepted that intelligence work is the most effective form of counter-terrorism, and that the best intelligence comes from community engagement, not coercion. The arrest in 2008 of Andrew Ibrahim for intent to commit terrorism followed tip-offs from Bristol's Muslim

community, for example. Detective work plays the key role in identifying terrorists after attacks – despite the oft-shown surveillance camera footage of the 7/7 bombers at Luton station, it was forensic examination of corpses and intelligence from the missing persons helpline that identified them.

What public evidence there is on anti-terrorist investigations demonstrates the overwhelming importance of community tip-offs and informants. One of the most robust studies concluded that information from these sources initiate 76% of anti-terrorist investigations. This analysis of 225 individuals recruited or inspired by al-Qaeda revealed that "the contribution of NSA's bulk surveillance programmes to these cases was minimal", playing an identifiable role – with the most generous interpretation of the results – in just 1.8% of cases. The vital importance of traditional investigative and intelligence methods is undeniable.

Getting priorities right

A recurring problem is prioritising and analysing the information already collected. It's no longer remarkable to discover that terrorists are already known to police and intelligence agencies. This was the case with 7/7 bombers Mohammed Siddique Khan and Shezhad Tanweer in London, and some of those thought responsible for the Paris attacks, Brahim Abdeslam, Omar Ismail Mostefai and Samy Amimour.

Questions are rightly asked about lost opportunities to apprehend them before they could kill, but this does at least indicate that intelligence-gathering is effective. What it also shows is the problem of prioritising information, and acting on it, particularly when there is an enormous amount of information to process.

Surveillance scholar David Lyon in his analysis of the Snowden

revelations suggests that 1.2m Americans are under surveillance and considered a potential terrorist threat. Notwithstanding debates over proportionality and the reach of such activities, such an enormous number suggests there's already sufficient surveillance capacity among the surveillance agencies. It's the ability to properly scrutinise what they learn and make use of it that's needed – not powers that would allow them to collect even more.

As contemporary philosophers of science have consistently argued, the physical and online realms are intrinsically yoked together. It makes no sense to suggest that surveillance of digital communications and internet use is something de-personalised that doesn't infringe an individual's privacy. These are claims made to soften the vocabulary of surveillance and excuse the lack of consent or proportionality.

So we must be wary of the evangelism of those pushing technological solutions to security problems, and the political clamour for mass surveillance. There are practical and cost considerations alongside the debate around the ethics of mass surveillance and its effects on privacy, consent, data protection, the wrongful characterisation of innocents as suspects, and the potential chilling effects on free expression. As mechanisms for collecting data become more opaque it becomes increasingly difficult to hold the agencies responsible to account and assess whether the social costs are worth it.

Source: The Conversation

https://phys.org/news/2015-11-opinion-paris-traditional-safe-mass.html