Secrecy, distrust, and interception of communications

LSE PhD researcher Bernard Keenan breaks down the different elements of the concept of "secrecy" that were highlighted by the recently-released report on surveillance laws in the UK.

The long-awaited report from the Independent Reviewer of Terrorism Legislation, David Anderson QC, was published on 11 June. Entitled 'A Question of Trust', it is the first comprehensive and politically impartial official review of the complex legislative framework governing interception-of-communication powers in the UK. This post does not discuss the content of the report in great detail. Instead, drawing on the work of Eva Horn on political secrecy, it frames the issue of trust by comparing three very different meanings implied by the English word 'secrecy'. The three senses derive from Latin. The first is *arcana imperii*, implying political techniques that are inherently secret; the second, *secretum*, refers to something that has been separated or divided; while the third, *mysterium*, refers to transcendental truth that can only be revealed by God. All play a part in this story.

Arcana

The power to intercept communication is one of the *arcana imperii*. According to Tacitus, these 'secrets of the Empire' are political techniques which are by their very nature secret. If openly discussed, they would be rendered useless, endangering the state. Fundamental to the operation of political power, the *arcana* are techniques according to which sovereign power is defined and exercised. In England, as long as there has been a formal system for writing down information and sending it elsewhere, the Crown has exercised the power to secretly read it. The postal system and all subsequent infrastructures for transmission of information were designed to allow for state interception. Insofar as law was concerned with these practices, it was traditionally used to protect the Crown's monopoly, not restrain their use. The law of England did not recognise a right to privacy over communication. So although a requirement for a ministerial warrant to open letters was first introduced in 1663, the aim was to ensure anyone other than the state who opened letters did so illegally. During times of war, general warrants were issued for the interception of *all* letters addressed to enemy territories.

The use of such practices became a matter for Parliament only following rare political scandals – a short list that includes names like Mazzini , Malone , and now Snowden – and even then, individual cases were never discussed in detail. Otherwise, the efficacy of the powers would be negated.

What is new is the attempt to limit it by law; an enterprise that only truly began in 1985 following decisions of the European Court of Human Rights. Yet as Anderson shows, the Interception of Communications Act 1985 and the subsequent Regulation of Investigatory Powers Act 2000 failed to adequately address or constrain the scope of executive power to intercept communication. Historically speaking then, what Anderson now proposes is novel and ambitions. But more than that, *arcana imperii* remind us that there is no perfect answer to the problem. Public law operates by publicly constraining the scope of the exercise of public power, but interception powers belong to a class of powers that by definition cannot be made fully visible to the public. The public is, by definition, set apart from the tasks that are conducted in their name.

Secretum

This engages the second sense of secrecy, *secretum*. Secretum is that which has been divided. From the beginning, the etymology of 'secret' in English directly signals a form of relationship that exists between the two parts of something divided. In this case, the division is between those who know and everyone else. Crucially, the division itself is no longer secret, if it ever was. Today, we who do not know *know that we do not know*. Every schoolchild who has seen two friends whispering about them knows this feeling. But for democracies, *arcana* represent an obvious problem: by holding back the most important political information, secret techniques stand in opposition to the very idea of the public as the ultimate decider. The suspicion and political distrust that this inevitably creates is that of being set apart, of *secretum*.

Anderson's report has been welcomed by the government insofar as he does not propose strong limits on the capacity of the state to collect and store information in large quantities. Against that, civil liberties campaigners welcome the proposal that the line between openness and closure ought to be shifted. Anderson wants an independent judicial body to scrutinise applications for interception warrants, shifting the power away from ministers and into the hands of formally independent judges. The government is certain to oppose this. Yet it will be a heated argument. Ministers are theoretically accountable to Parliament, but Parliament has no specific information with which to question their decisions. Governments proffer nothing and 'neither confirm nor deny' any specific questions. Independent judges, on the other hand, are used to dealing with the legal repercussions of decisions that affect protected rights, and have a professional duty of scepticism, to ask questions of those who want permission to spy. A division of the power to authorise would be a vast improvement. Yet we must also acknowledge that bringing judges into the fold will not simply engender trust. It will also make those judges concerned the targets of mistrust. The division will persist, but the dividing line will be redrawn. Anyone concerned with protecting privacy and curtailing the arcana of state should campaign for Anderson's judicial body in the strongest possible terms. Yet at the same time, we must also recognise that when dealing with secrecy, what is at stake is not so much a system of trust as a means of managing distrust.

Mysterium

Mysterium is best understood in the religious sense. A mystery is the idea of a transcendental truth, attributed to God or the divine. As such, it is only revealed through divine signs, and its truth cannot be second-guessed by humans. It stands in opposition to the axioms of scientific modernity. Therefore *mysterium* seems to have little application to the technoscientific world of digital communication. But, as systems theorist Elena Esposito has pointed out, the concept is helpful for thinking about the consequences of the 'big data' revolution that we are living through. In relation to interception powers, a key part of Anderson's report recommends retaining bulk collection powers and retention of internet traffic data. In relation to investigative police work, the point is obvious: a criminal investigation can make use of records showing the movements or interactions of suspects or victims after the crime. As no one can predict who will be a suspect or a victim, it is necessary to retain records on everyone. The type of information and storage duration are up for debate.

But when it comes to intelligence, we are looking not to the recent past but into the future. Rather than proving facts, collected data can be used to make predictions. Patterns derived from crunching 'big data' are already transforming decision-making in commercial, medical, and scientific systems. The promise for intelligence agencies is similar: the more data that is made cheaply available, the more correlations can be observed, tested, and refined by 'smart' algorithms; the more accurate the machine predictions of future behaviour will become. The digital environment promises that interception of communication will lead to interception of action – terrorist action, criminal action – *before* it happens. This requires that all communication, including that of innocent people, is made potentially available for analysis. The scale of calculation is such that only the machine can compute the risks and order human intervention – as with *mysterium*, human minds will not have the capacity to second-guess the decisions. But machines are not God. Data is structured by human coding and algorithms are biased towards certain selections. Indeed, that's what makes them effective.

We already live in a world in which pre-emptive computing is implicated in helping humans make important decisions. In the field of state surveillance, we need to build on Anderson's report so that privacy is not seen only as relating to interception of information, but also how that information is processed and used in political decisions. The line between secrecy and openness cannot be done away with, but where it is drawn is crucially important.

This post gives the views of the authors, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

June 22nd, 2015 | Featured, Filtering and Censorship, Guest Blog, Internet Freedom, Internet Governance, Privacy | 1 Comment