A very brief history of interception

Britain is in the process of legislating a new system of control over the interception of communication. The Investigatory Powers Bill, currently being debated in draft form, aims to give an unprecedented level of transparency and accountability to the use of government surveillance powers. In this 'long read' piece for the Media Policy Project, LSE PhD student Bernard Keenan provides some historical context on the issue of interception, arguing that the more the law oversees secret activities, the more secretive the law becomes.

The prerogative phase 1634 – 1984

In 1635, the English Royal messenger service was opened up to public use. It would evolve into a crucial aspect of the modern world. Scientific learning, philosophical investigation, long-distance trade, even literary culture and news media all arose in part thanks to the material affordances of the postal service. Just as the printing press became society's mechanical memory system, the postal service provided a reliable and profitable system for disseminating written communication across time and space.

Simultaneously, the centralised postal system made this emergent 'public' transparent to another recent development: the intelligence apparatus of the state. Centralised control over written letters meant that a new order of knowledge about crime, political conspiracy, and foreign threats to the realm could be smoothly and secretly obtained, giving rise to new strategies for gathering intelligence, disrupting plots, and prosecuting crimes. From 1657 onwards, the only legal control over this practice was that no one could open a letter in transit except under the authority of a warrant issued by a government minister. These warrants were not to control the use of the power by the government; rather they were to ensure that anyone who interfered with the post without a warrant could be prosecuted. The content, shape, and form of such warrants were outside the realm of legal decision-making, and the system operated in near-total secrecy. Interception itself was authorised under the prerogative powers of government – the government saw itself as free to decide what to do in such matters.

Save for occasional political scandals in the 19th and 20th centuries, secrecy was well maintained well into the age of the telegram, telephone, and even into the early days of the digital revolution. The brief interception scandals of the 1840s and 1950s were dealt with by a most British method for diffusing scandal and brushing it under the carpet with minimum disruption: Parliamentary Inquiry. Formally, the government persistently refused to either confirm or deny interception practices took place (indeed, it was during the Mazzini scandal of 1844 that a government minister first refused to confirm or deny a question in Parliament). Legally, the courts in England avoided making any decisions on interception powers at all.

This persisted until an antiques dealer, Mr Malone, forced the issue in the High Court in 1979, after the police accidentally revealed that they had been tapping his telephone line. The lawyer for the Metropolitan Police took the usual government line, maintaining a formal silence on the facts. The High Court therefore treated the matter hypothetically and concluded that even if Malone had been tapped (which he had), it couldn't have been unlawful because there was no legal right to

privacy in England's common law, and hence that there could be no problem because the government could do anything – anything at all – provided that it didn't interfere with a legal right.

The obfuscation phase 1985 – 2015

Malone took the matter to Strasbourg, where the European Court of Human Rights (ECtHR) found that this situation was untenable. From Strasbourg's point of view, Article 8 of the European Convention on Human Rights (ECHR) had granted the people of the UK a right to private life since the UK had signed up to the Convention over 30 years before. The Court found that interception powers interfere with privacy; this could only be lawfully done if a public law were in place. Such a law would let people know – at least to some extent – the circumstances in which their privacy rights might be violated. To be compatible with Article 8 of the ECHR, any such interference under the law is only permitted if it is both necessary and proportionate in the context of a democratic society.

Although this was 15 years before the Human Rights Act 1998 domesticated the ECHR, the ruling nonetheless resulted in the Interception of Communications Act 1985, a thin piece of legislation that did the minimum required by the *Malone* judgment, and gave practically nothing away about the type of powers used by the police and intelligence services. Perhaps this sounds cynical, but we should also remember that the 1985 Act was a usefully timed piece of administrative law. Coming around the same time that the Thatcher government began selling off state-run enterprises, the Act ensured that the new companies about to take over the newly privatised telecoms market such as British Telecom and Mercury would have to allow the state to maintain existing interception powers – and to respect official secrecy. It respected human rights law in form, but in retrospect it was also a practical response to the coming digital age.

The 1985 legislation was replaced with the Regulation of Investigatory Powers Act 2000 (RIPA), a now notorious piece of lengthy and confusing legislation that appears in retrospect to have been drafted so as to be deliberately obfuscatory as to the nature of the powers that it implicitly authorised. A handful of investigative journalists and technologically sophisticated observers, such as Duncan Campbell, drew attention to this, but it was the global impact of Edward Snowden's disclosures in 2013 that led to revelations about the nature and extent of activity that RIPA ostensibly allowed. Mass collection of internet traffic, database collection from Internet Service Providers and other sources, 'bulk' analysis techniques of information pertaining to innocent people, compromising digital security systems around the world, intelligence sharing with the United States and other allies, and hacking into organisations in friendly countries. Such alleged activities were never authorised by Parliament, and they stretched the interpretation of the provisions of RIPA and other obscure pieces of legislation to breaking point.

What is most disappointing is that prior to Snowden's disclosures, neither the surveillance court first set up to hear complaints from individuals in 1985 (enhanced in 2000 to the present-day Investigatory Powers Tribunal), nor the Interception of Communications Commissioner who oversee such powers on a day-to-day basis were fully aware of the extent of these activities; or if they were, they did not understand them to be incompatible with the governing legislation.

2016: the transparency phase?

Edward Snowden and pro-privacy organisations have started a conversation that has – not accidentally – coincided with a growing awareness of the unprecedented ways that life lived online renders us transparent to both private companies and state actors. Both as individuals and as groups, we can be categorised, profiled, and influenced in ways that we cannot easily understand, based on decisions that are increasingly machine-led. It is a cliché by now, but in this context it bears repeating that the digital revolution is as big a transformation as print-plus-post was during the early modern period – and it is happening at a much greater pace. At the same time, we must accept that security threats come no longer solely from nation-states. There remains a legitimate need for secret intelligence techniques that government and law enforcement can use.

We are putting in place a legislative control system the principles of which will frame the understanding of interception powers for a long time. There are obviously risks on both sides of the debate. Risk permeates the discussion, and it is inevitable that the only thing we really know about tomorrow is that it will be different from today. It is worth not rushing this debate, and it is worthwhile getting involved in the next round of Parliamentary scrutiny, when it opens, if you have a view on these questions: like it or not, we all will be affected. Detailed clause-by-clause breakdowns of the draft Bill are available elsewhere, and each section in turn commands a great deal of debate.

In the past week both the Intelligence and Security Committee and the Joint Committee on the Draft Investigatory Powers Bill have reported publicly their analyses of the draft Bill. Both are critical of the structure and content of the draft as it stands. It seems clear that the legislation will be rushed through Parliament, as MPs and the mass media begin to understand the complexities involved.

(Provisional) conclusions

We are in the middle of things, so a couple of general theoretical observations must serve as a provisional conclusion. From a legal historical and theoretical position, there are perhaps two general points to make. The first is that the individual is no longer the only point of reference. Surveillance powers today have the potential to affect not just individuals but whole groups of people who might be categorised according to any number of characteristics suggested by their data. The argument that you yourself have 'nothing to hide' neglects this enhanced social dimension: what does it mean, for instance, if journalists cannot safely receive information from whistleblowers about abuses of power? Or if retained personal data – required under the draft Bill – were stolen or leaked, meaning your employer was blackmailed, or put out of business?

We should be honest in admitting that bulk dataset retention and collection as described in the Draft Bill effectively sets the conditions for mass surveillance. This does not mean that the entire population is *actively* being watched as individuals, as was the situation in the former East Germany; but it does mean that everyone's personal data is *potentially* figuring in some analytic process. It is difficult to square these concerns with the individual rights-bearing subject that the law traditionally protects, and with the ideals of political and economic freedom in a public sphere. Is it possible to think of group-based categories, which will nonetheless protect individual rights without giving rise to potential discrimination in this diffuse context? This seems to be an urgent question.

The second point is one I have outlined elsewhere on this blog. It goes to the heart of the idea of open justice and democracy. It is easy to take for granted the ideology of the public sphere: in democracies, we assume that the government is bound by publicly known rules, and that such rules are decided by elected representatives of the public and supervised by publicly open courts and independent observers. Yet this is self-evidently not the whole story. However noble or ignoble were their intentions and activities over time, the history of secret interception demonstrates that the public sphere, which supposedly constitutes the democratic state and permits us to trust it, has always been underwritten by a secret sphere acting in the interests of the state and out of public sight, both distrusting and distrusted. For centuries, the rule of law has managed to avoid confronting this reality head on, but no longer. We need to think about the extent to which the law can mitigate the loss of trust that it now risks. For the more the law oversees secret activities, the more secretive the law becomes.

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

February 15th, 2016 | Featured, Filtering and Censorship | 0 Comments