The government's proposal for data communications surveillance will be invasive and costly with minimal effectiveness

Blog Admin

The government has proposed providing law enforcement officials with unprecedented access to internet communications. **Joss Wright** *argues that this amounts to a hugely expensive and invasive scheme that will have only minimal effectiveness in achieving its stated goals.*

The means through which we communicate have undergone dramatic changes in recent decades. Mobile phones and Skype have largely superseded traditional telephones, emails are sent in place of letters and postcards, much of our news and information comes from websites and search engines, and technologies such as instant messaging, SMS, Facebook and Twitter are thriving in communication niches that barely existed twenty years ago. These changes have brought new opportunities and means of organising, both for legitimate and nefarious purposes. It is in the context of these advances that the coalition government has proposed to revive Labour's abandoned Interception Modernisation Programme, rebranded as the 'Communication Capabilities Development Programme' or CCDP. Put briefly, the CCDP has been presented as a means by which law enforcement and intelligence agencies are to expand their capabilities to monitor all forms of online communications. In doing so the scope of what will be intercepted and analysed, and the infrastructure required to support such surveillance, is to be massively extended. There are numerous objections to these proposals, based on the limited information to which we have access, and I will attempt to address the more significant of these.

One of the most worrying objections lies not in the proposals themselves, but instead in the lack of transparency that surrounds them. Despite the sweeping nature of the changes that have been implied, extremely little detailed information regarding the implementation of the policy has been revealed to the public. This has forced civil liberties campaigners, such as those who attended the recent LSE-hosted 'Scrambling for Safety' event, to extrapolate from the stated aims of the new proposals, from details of previous and existing schemes, and from known technologies. This has led, inevitably, to accusations from proponents of the CCDP that any criticisms are unfounded scaremongering.

When we examine what has been said about the newly-revived proposals, the most notable aspect of the rhetoric, as with earlier proposals under Labour, is the assertion that they are nothing new. Instead, we are repeatedly told, these programmes are merely a means by which law enforcement and intelligence services can 'maintain' or 'preserve' existing capabilities required for fighting terrorism. If our phone records are already subject to monitoring, what possible objection could there be to extending this to details of emails, web pages, social media, and Skype?

This argument relies on a fundamental misconception. Despite any superficial similarities between old and new communication technologies, it is both disingenuous and dangerously simplistic to consider access to phone records as a useful analogy for making policy about combined access to email, web, social media and other internet traffic. The extent to which we use these new services is vastly greater, the information that they reveal about our habits and interactions greater still. This is further amplified by the ease with which these separate records can be correlated and cross-referenced. A closer analogy than logging telephone calls is the noting of every conversation we have, every book or newspaper article that we read, every shop that we visit and what we buy, as well as a host of other interactions that together make up a frighteningly detailed picture of our life and habits.

Proponents are quick to point out that the content of our communications will not be subject to scrutiny; only 'communications' data will be logged. This includes details such as the name of websites, the sender and recipient of emails, and the time at which communications took place. This detail is often presented to alleviate concerns that the proposed monitoring would be in any way invasive. This, again, is either intentionally misleading or dangerously misinformed, flying as it does in the face of many decades of research and application of traffic analysis — the inference of details purely from patterns of communications. As the proposals themselves show, this technique is considered to be a powerful tool in analysing individuals for criminal or terrorist activity. It is equally powerful and revealing about our own daily habits, and presents a deep and unacceptable intrusion into our right to a private life.

Neither is it true that communications data is simple to differentiate from the content of communications. In modern online services the distinction between communication and content has blurred to an extent that can often leave it meaningless. This can be demonstrated with the example of visiting a website: it is easy to see that the URL 'google.com' is distinct from the page of search results that you see when querying the site. In reality, however, a Google search for 'government surveillance' will result in a URL more akin to 'http://www.google.com/search?q=government+surveillance'. With the search terms, and potentially other identifying information, so prominently highlighted, should this be considered communication or content data?

In fact, this battle was fought and won by the Foundation for Information Policy Research in 2000, with an amendment to the Regulation of Investigatory Powers Act to limit communications data to the first slash ('/') in URLs, revealing only 'google.com' and discarding all other information. While this seems an easy distinction, the situation is complicated in many current services, including Google and Facebook, in which all interactions take place through the website. If this distinction between communication and content data is upheld, it would prevent monitoring of anyone communicating via Gmail or Facebook messages, unless the companies themselves provide internal access for monitoring. It therefore seems likely that, in the interests of 'maintaining current capabilities', any such restrictions would necessarily be repealed or bypassed.

Returning to a familiar point of contention, there is much concern over the treatment of encrypted communications. Many modern services, again including Google and Facebook, use encrypted connections by default for purely practical security reasons. In order to gain meaningful communication data regarding, for example, messages between Facebook users, monitoring equipment will have to be installed within the organisation itself. This raises a vast range of questions concerning jurisdiction, oversight, cost and compliance: who will pay for this monitoring equipment, who will install and maintain it, who will ensure its correct and legal use, and how will individual companies respond to such compulsion? These concerns were recently dismissed by the Home Secretary, in answer to a question from the Home Affairs Select Committee, as 'a technical detail'.

The costs and benefits of such a scheme are, of course, serious considerations. The earlier Interception Modernisation Programme was projected to cost £2bn over ten years, and experience with government IT programmes suggests that the final cost is likely to be much higher. More seriously, the scheme will not be effective in identifying criminal or terrorist activity due to the inevitable inaccuracies and misclassifications that arise from analysing populations on a national scale; the sheer volume of data simply overwhelms the analysis. This is not a limitation on current technology that can be solved with faster computers and larger databases, but the inevitable result of analysing vast quantities of data. Such a system would, it is true, present insight into the activities of those who are already under suspicion but would be largely useless for identifying threats, and would do so only at the cost of providing equally invasive details on the entire population. Controlling access to this information would be impossible, as we see from existing data breaches and abuses. We are therefore presented with a hugely expensive and invasive scheme that will have only minimal effectiveness in achieving its stated goals, but be a serious risk to our privacy.

As with all such schemes, the proposed regime of surveillance presents a grave risk of use and abuse beyond their stated purpose. Deep packet inspection, or DPI, equipment of the type required by the CCDP inherently possesses the capability to monitor both content and communications data, and will necessarily be installed on a vast scale. That only the appropriate data will be accessed relies purely on

guarantees that are impossible to verify, and that cannot be guarded against changes in policy or institutional misuse. We have only to recall local councils abusing RIPA powers to check if parents fell into appropriate school catchment areas to imagine the kind of day-to-day abuses that are made possible. Nor is it in any way an exaggeration to compare the infrastructure that such surveillance proposals require to those that were used recently to such devastating effect in Syria — indeed, they are likely to be the same pieces of equipment, developed by the same Western companies.

While the above arguments have focused to some extent on technology and the risks that come with its misguided application. A more important and fundamental argument, however, is that the proposed approach follows and accelerates a worrying trend towards blanket and unwarranted surveillance of the population in the hope of identifying those who may commit crimes. With the wealth of information revealed by communications data, the appeal to a Home Secretary of an algorithmic black box that can magically identify terrorists is, perhaps, understandable, at least to those unfamiliar with the concept of the base rate fallacy; such a view, however, violates the basic principle that individuals for whom there is no evidence or suspicion of wrongdoing should not be targeted. Without this principle, where does the surveillance and intrusion into our lives end?

There are many arguments against surveillance of the type proposed in schemes such as the Communication Capabilities Development Programme, and I have touched on only a fraction. In the past, technical and economic feasibility, as well as compliance with EU law, have proved some of the most powerful of these arguments, and they will remain so. Despite this, I believe that our arguments should stem first and foremost from the fact that blanket and unwarranted surveillance of the population is deeply wrong, both in terms of our fundamental human rights and in our most basic values as a society. Until that argument is won we will never see the end of these misguided and damaging proposals.

Please read our comments policy before posting.

Note: This article gives the views of the author, and not the position of the British Politics and Policy blog, nor of the London School of Economics.

About the author

Dr Joss Wright *obtained his PhD in Computer Science from the University of York in 2008, where his work focused on the design and analysis of anonymous communication systems. Dr. Wright has provided advice to the European Commission, as well as a number of EU research projects, on the social, legal and ethical impacts of security technologies, and has also written articles on privacy, social media and online activism for the Guardian and Observer, amongst others*

You may also be interested in the following posts (automatically generated):

1. Book Review: One Nation Under Surveillance (20.5)
2. Facebook's 'dirty tricks' campaign against Google will have unexpected consequences in relation to the way that personal data is used and abused (15)
3. Behind the WikiLeaks furore, there's a much bigger issue at stake: America's slack approach to information security. The UK national interest lies in demanding that the USA act to stop its government computer systems being breached time and again, and in reviewing British data security as well. (13.1)