

0 Introduction

The stated aim of the NSA and GCHQ is to be able to command access to any and all electronic information available from public networks. GCHQ's strategy for controlling worldwide online communications is termed, "Mastering the Internet"ⁱ. This means being able to access and collect all forms of information, from every possible digital communications channel to acquire, "all the signals all the time"ⁱⁱ.

There is little new information in this report. It gives an overview of what we have learnt from disclosures in the Guardian, Der Spiegel, New York Times and more recently The Intercept.

Many of these activities were unknown until Edward Snowden's leaks started to be published in 2013. The government has largely refused to acknowledge the programmes and activities described, merely asserting that all surveillance conducted in the UK takes places in accordance with the law, under warrants issued by secretaries of state.

The official supervisory mechanisms, such as the Intelligence and Security Committee, have also asserted that little needs to change, and that oversight in the UK is exemplary. Nevertheless, as this report shows, there has been strong indication that, prior to Snowden's leaks, oversight bodies had no real idea of what was taking place.ⁱⁱⁱ

There has been no serious questioning by the official Opposition in Parliament, which despite calling for a public debate has yet to define its own position to the revelations. The Government for its part has responded not just with silence, but by demanding new powers of acquisition for personal communications data.

The UK has been denied a thorough public debate. It has to be said that most of the British media have not picked up on public disquiet, reflected in polls saying people want a debate, but have rather responded to Government calls to limit what they perceive as damage caused by the mere fact of public knowledge about surveillance programmes.

There are several inquiries running into aspects of the UK's surveillance programmes. New evidence of specific disquieting activities continues to emerge. There are also a number of ongoing legal challenges, which are helping to shed light on secret surveillance practices. These include cases brought by Privacy International, Liberty and Reprieve, who have taken the government to the Investigatory Powers Tribunal. One result of this is that evidence of procedures and policies has become public, so we have an understanding of the government's internal procedures for some of the programmes.

Further information will come to light through court cases, including Open Rights Group challenge at the European Court of Human Rights as part of the Privacy not Prism coalition. This case means that the UK Government will have to respond to the allegations and explain how GCHQ's blanket surveillance regime is foreseeable in law, and necessary and proportionate.

No one would deny that surveillance is a tool that governments must use to fight terrorism and serious crime. The intention of this report is to support this work. But even if the job they do aims to keep our country safe, the intelligence services still need to be accountable at some level to Parliament and to the public. We cannot simply take their word for it.

What, then, should our Parliamentarians, political parties and Government be seeking to change? Is the current slow pace of reform adequate? Is it reasonable to suppose that, once media revelations diminish, the security agencies can simply return to business as usual, or that the unease created by the Guardian revelations can be answered by creating political demand for new surveillance powers? What are the remaining implications of the revelations: is the major consequence actually behaviour change among

terrorist suspects, as alleged by security chiefs? Or are there wider questions that must be considered? These are the questions we try to answer in this report.

0.1 About this report

Part 1 of this report give a broad overview of GCHQ's activities, looking at the range of data that is being harvested in 'passive' collection, invasive methods used to collect data and how the security services' mission has expanded from passive collection to offensive capabilities. We also look at how data is processed, stored, analysed, accessed and shared with international partners.

Part 2 analyses how the legal regime has permitted these activities to take place and where the loopholes are being exploited. We believe that the law needs to spell out the capabilities and powers that GCHQ have, which it currently does not do. We also examine the problems with current oversight mechanisms, and where they are failing to hold the security services to account. Finally, we document the full set of threats and the kinds of approach to risk management that should be taken.

Each of GCHQ's programmes and data sharing arrangements has a complicated set of costs, effects, risks and alleged benefits. The negative effects start with the impact on everyone's right to privacy but extend much further. There is a basic question of risk management in order to understand the potential external impact, as well as questions of legality and ethics. This of course is extremely important work which needs to be undertaken by any oversight body.

We examine the threats to democracy, social cohesion and rights such as freedom of expression, which have been undermined by revelations of surveillance against lawyers, journalists and activists. GCHQ's activities have profound implications for every business that depends on information technology and are capable of inflicting serious damage to cyber security, trust and the economy – the effects being felt domestically and overseas. They also have implications for our foreign standing and could pose a threat to their own aims.

The aim of this report is to encourage Parliament and the Executive to consider the full cost benefit analyses of surveillance. We also recommend ways that the legal regime and parliamentary oversight need to be reformed. With more transparency, accountability and proportionality, we believe that the public will have confidence in the work of the security services. The alternative is to allow the security services to 'master the Internet', causing us to lose the freedom and rights that they are here to protect.

0.2 About GCHQ

GCHQ is the UK's signal's intelligence agency. Over the past 20 years, GCHQ has come out of the shadows of the cold war, when its existence was not even acknowledged, and is slowly being integrated into the wider civil service.^{iv} But at heart it remains a secretive organisation with little public accountability.

GCHQ operates on three fronts. At the domestic level, GCHQ provides support with interception and recovery of encrypted data to a broader range of Government bodies for law enforcement, through the National Technical Assistance Centre (NTAC). NTAC was transferred from the Home Office to GCHQ in 2006, and serves the UK intelligence and security agencies and police forces, as well as HM Revenue and Customs (HMRC) and the National Crime Agency (NCA).

GCHQ is also responsible for the CESG, which is the UK's National Technical Authority for Information Assurance (IA) – responsible for ensuring that information systems used in the public sector are properly secured.^v

In parallel, GCHQ works as a classic external spy agency responsible for strategic intelligence, looking for potential threats and opportunities in a world of realpolitik normally hidden from the public, where even allies such as Belgium are legitimate targets.

GCHQ and UK Mass Surveillance

The international side of GCHQ involves working with the UK's Secret Intelligence Service, MI6, and the military. Critically, GCHQ also operates very closely with the US National Security Agency (NSA) and the other partners in the Five Eyes alliance of signal intelligence agencies (Australia, Canada, New Zealand, the UK and the US). This involves extensive sharing of information, techniques and resources through a series of secret agreements.

-
- i This name was first aired by The Register and the Sunday Times in 2009, but at the time it was deemed to describe what was to be called The Snooper's Charter system of internal surveillance within the UK. The articles did not mention the existing mass surveillance nor the US connection. http://www.theregister.co.uk/2009/05/03/gchq_mti/
 - ii <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>
 - iii For instance, <http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm>

Mr Watson: I am reassured by my right hon. Friend's thoroughness in the investigation. Was July the first time that the Committee had examined Prism, and was that after the *Guardian* revelations? *[Laughter.]*

Mr Howarth: It was after the *Guardian* revelations. The hon. Member for Cambridge seems to think that that is funny. Actually, he would still be sitting here today if we had not gone and looked at this matter after the allegations emerged. He would be accusing us of being inadequate in our responsibilities.

- iv <http://www.civilservice.gov.uk/wp-content/uploads/2011/09/GCHQ-phase2-July2009.pdf>
- v <http://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx>