Submission to the Privacy and Security Inquiry

Christopher Foy[i]

29 January 2014

1. The layered revelations about the invasion of privacy of British and other citizens by GCHQ and the NSA have revealed an extraordinary tipping of the balance against the rights of citizens for privacy in the direction and content of their communications, towards the indiscriminate harvesting and swapping of data by government agencies, for which there is no criminal (or reasonably criminally suspect) justification. The publication of the reports that now inform this debate around the world is most welcome. And doubtless we can look forward to even more insight in the months to come.

2. The pendulum between the rights of the citizen and the responsibilities of the state is plainly stuck at the wrong end of its arc. Adducing the comfort blanket of generalised security concerns and enjoying close relations with 'friends across the pond' can in no circumstances justify the suppression of the fundamental and general right to privacy of British citizens.

3. In the context of the breadth of information in the public domain about the secret acquisition of personal data by government agencies, if it can be objectively demonstrated that *in every regard and in every instance* the capture, management and manipulation of British citizens' private communication data by the security agencies has *always* complied with British and international law, then that law is plainly no longer fit for purpose. The right to be spied upon without reason has not been – and is not now being - delegated to its government by British citizens.

4. The failure of the law to properly protect rights to privacy and the existence of technology that makes possible the widespread gathering and interrogation of limitless quantities of private communication data both require that the individual right to privacy should be freshly affirmed in terms that effectively protect citizens from breaches by government and its agencies and its allies. And since the technology of intrusion can be expected to become increasingly potent, the protection of citizens' rights must be framed unambiguously not only to address the present state of affairs but, insofar as it is possible, to anticipate future developments. It must then be kept under regular review and updated as necessary in the light of technical developments.

5. One of the slender means by which citizens can partially protect themselves is encryption. The reports of steps taken by British and US agencies deliberately to weaken encryption systems represents an attack on all users, from which their agencies and organized crime alike benefit. Government should be directed to reinforcing continuous improvement in failsafe and accessible encryption; and developments should be given maximum research support.

6. Where there is evidence of criminal behaviour and/or criminal intent, including terrorist acts, that is derived from means that do not breach rights to privacy, specific measures of intrusive enquiry may be warranted. Each case must be subject to equally specific judicial pre-approval. If circumstances were to warrant emergency intervention then equivalent judicial approval must be sought without delay, straightaway afterwards. Authorization must never be delegated to the politicians who are accountable to parliament for the conduct of relevant agencies.

7. A question clearly arises as to whether the Intelligence and Security Committee may itself be too closely identified with the associated security agencies to be able to promote an objective recommendation on relevant new legislation. Answering this may entail judicial and/or public review to ensure that ineradicable principles are not jettisoned by stewards who are parti pris.

[i] This statement is made in a personal capacity by Christopher Foy of [REDACTED]