Submission to Intelligence and Security Committee of Parliament: Privacy and Security Inquiry

Executive Summary: The fundamentally different nature of digital data (things like emails, Web pages and metadata) compared with analogue equivalents (letters, books, telephone numbers) requires a very different approach to the collection, monitoring and interception of private communications.

1. My name is Glyn Moody, and I am making this submission in a personal capacity based on my professional knowledge and experience. I have two degrees in applied mathematics from Cambridge University, including a doctorate, and have been a technology journalist for over 30 years. I began writing about computers in 1982, and about the Internet, surveillance and encryption in 1994, and continue to explore all these areas in my writing. My work has appeared widely online, in magazines, and in publications such as The Economist, The Guardian and The Daily Telegraph.

2. To answer the question about striking a balance between the individual right to privacy and the collective right to security, I would first like to note that our society is undergoing a technological shift so profound that it is not "once in a lifetime", but literally "once in a civilisation".

3. This is the shift from analogue information, stored in physical objects like books, LPs, tape cassettes, celluloid films etc. where the medium is an essential part of the artefact, to digital information, which is stored as a series of 0s and 1s on a multitude of different media whose details are largely irrelevant. That shift only takes places once (assuming that there are no discontinuities in civilisation itself), as analogue knowledge is converted into digital forms through scanning, re-typing etc. Once in that form, it can be copied endlessly, and for almost zero cost, thus allowing multiple copies to be made, and avoiding the need to digitise again.

4. That profound change touches all aspects of modern life. It means, for example, that we are fast approaching the point where we can store every book, every picture, every film, and every recording on a single device (for example a hard disc or solid state storage). Not only will it be possible to place all human knowledge in the palm of your hand, it will be possible to make endless copies of it for zero cost (although copyright issues are likely to prevent that happening.)

5. Computing power continues to increase year-by-year. This is generally encapsulated in what is known as "Moore's Law", which states that, roughly speaking, for a fixed cost, computers double in power every 18 months; or, equivalently, the cost of a given computing capability halves every year and a half. Because this is compound growth, the effects over time become very large.

6. To give a concrete example: according to Google, a single online query made with its search engine uses as much power as all the computing done throughout the planning and execution of the 11-year, 17-mission Apollo space programme.

7. Alongside advances in computing power, computing storage has also become more powerful and cheaper, allowing progressively larger quantities of digital data to be stored. A former NSA technical director, William Binney, estimates that one NSA data centre currently being built in Utah will be able to handle and process five zettabytes of data – five million million gigabytes. To give an idea of what that means, we could imagine printing out the NSA's information as paper documents, and storing them in traditional filing cabinets. Doing so would require around 42 million million cabinets occupying 17 million square kilometres of floor space.

8. That figure begins to hint at why the transition from analogue filing cabinets to digital storage is so important. Even if security services had the resources to gather private information about citizens that filled 42 million million filing cabinets, there would of course be no way to find anything again because of the immense scale. Moore's Law means that not only can any piece of digital information be found in millionths of a second using computers, but that any piece of information in any filing cabinet can be cross-referenced with every other piece of information in all of the 42 million million filing cabinets in order to look for interesting correlations or patterns.

9. This makes the large-scale gathering of communications metadata practised today by UK intelligence agencies extremely dangerous. Contrary to some claims, metadata is not less personal than the actual content of messages: in the digital age, it is actually far more revealing.

10. The contents of communications such as telephone calls or emails need to be broken down into their conceptual parts - that is, understood - before they can be used, and for the moment computers are still quite bad at that. That's why humans are needed to listen to conversations in order to understand properly what is being spoken about. That, in its turn, places a limit on how many conversations can be monitored in this way.

11. Metadata, on the other hand, is already broken down into conceptual parts – time, date, location, caller, recipient, etc. It can be analysed immediately and automatically by computers, and cross-referenced with those virtual 42 million million filing cabinets of other data held elsewhere.

12. This allows a complete map of a individual's life to be constructed – a four-dimensional map, since it includes past and present data to create a vast and detailed profile of everywhere that person went, everyone they met, everyone they called, every Web site they visited etc.

13. Moreover, the power of computers means that it is possible to extend the spider's web of connections to find out all these same things about the people they met, creating a widening circle of detailed information that together begins to form a complete representation of society, its constituent individuals and all their personal, economic and political relationships.

14. To show why this is both new and troubling, it is helpful to consider the use of closed-circuit television cameras (CCTV), which have become a familiar but not uncontested part of British life. However many million CCTVs there are, there intrusiveness is limited by virtue of the fact that they require people to look through recordings (automated systems exist, but are still vastly inferior to trained professionals.) Importantly, CCTV has only very limited metadata – things like geographical location and time of recording.

15. Contrast this now with the collection of "innocent" communications metadata. This instantly reveals who is communicating, and with whom, and often about what. It also brings with it a virtual crowd of people that hover around every individual – not in the physical world of CCTV images, but in the digital world of related data: their families, friends, acquaintances. It's like having a CCTV camera that knows and can store the name of everyone in its field of vision, their relationships, and what they are talking about.

16. But the key difference here is that this "digital CCTV" is not restricted to public places: it follows us into our homes, as it continues to track the emails and the text messages we send there, the Web pages we visit, the online purchases we make. It follows us into the doctor's surgery and hospital, where our previous Web searches will make it quite clear what our health problems are; and this all-knowing "digital CCTV" even records us in the bedroom, since metadata makes it

trivial to establish social relationships between any two people – including illicit ones.

17. The scope for abuse is immense. As we've seen in the recent revelations about systemic corruption in the Metropolitan police, no organisation is immune to this, however high its professional standards, and however great the trust placed in its probity. Where there is scope for abuse, there will be abuse. Particularly troubling is the prospect of people in positions of power – politicians, for example – being blackmailed. Buried in the stored metadata, ready to be excavated with increasingly powerful digital search techniques, are the most personal details of their lives, the most intimate patterns of their existence, and the facts they least want revealed.

18. It is not possible to stop computers becoming faster and more powerful, or to prevent database storage becoming cheaper and more capacious. The only way to prevent ever-deeper intrusions into our private lives – and ever-greater risks that unauthorised access will reveal our greatest vulnerabilities – is to limit the gathering of "innocent" communications. The less that is gathered, the harder it will be to intrude on the privacy of ordinary citizens, and the better-protected we will all be against revelations that threaten marriages, careers or even lives.

19. Scaling back such metadata gathering would not, of course, apply in situations where in-depth analysis of social relationships is vital and justified – when fighting terrorism or tackling serious crime etc. But those must become the exceptions, not the norm. They need to be strictly regulated, with full judicial oversight on a case-by-case basis to prevent vague or lax rules being circumvented. Although security services may lament the loss of the wider net that conveniently captures everybody's metadata, that will be offset by the constantly increasing computational power that can be brought to bear on the smaller, more relevant dataset. Moreover, to borrow the favourite metaphor in this context, it is far easier to find needles in a smaller haystack, than in a huge one. If such a system is implemented correctly, there need be no loss of collective security, but there will be a huge gain in proportionality and individual privacy.

20. My understanding is that surveillance in the UK is largely governed by the Regulation of Investigatory Powers Act 2000. Since this was drawn up a decade and a half ago, it is not surprising that it is wholly unable to address the new issues that I have raised above. It was drafted in a world that was still largely analogue, and its measures are designed to oversee the kind of activities that were common at that time. For example, it pre-supposed that surveillance was a one-off, time-intensive activity, and that general oversight was enough. That is no longer the case: surveillance today is automated, occurs almost instantly and on such a scale that blanket authorisations can no longer control it.

21. In the light of this, I would like to urge the Committee to press for a thorough review and complete revision of RIPA to make it fit for the digital age. The central element of this would be to forbid the blanket collection of "innocent" communications in the UK by the intelligence agencies, and to move to a system of highly targeted interceptions that must be individually approved, and that are subject to strict and meaningful oversight on a continuing basis. Failing to do so is likely to have profound consequences for privacy and liberty in this country because of the immense changes being wrought by the shift from analogue to digital technologies.

Glyn Moody

London