Submission to ISC Privacy and Security Inquiry

Professor Peter Sommer

Summary

I suggest an emphasis on extent, authorisation for, subsequent management of, and the provision of full audit trails of ***means of intrusion*** *rather than attempting to modify and update the existing and complex laws which seek to balance privacy and security.*

1. This is a personal submission.

2. I am currently a Visiting Professor at the CyberSecurity Centre at de Montfort University and a Visiting Reader at the Open University. For 17 years I was first a Visiting Research Fellow and then a Visiting Professor at the London School of Economics specialising in Information System Security. At the OU I am the Course Consultant for a Masters' course module on Computer Investigations and Forensics. I validated the UK's first computer forensics Master's course at the Defence Academy (Cranfield University). I am currently teaching a digital forensics course at the Cybersecurity Centre for Doctoral Training at Oxford University. During its existence I was the Joint Lead Assessor for the digital specialism at the Council for the Registration of Forensic Practitioners, In 2008 I was appointed to the Digital Forensics Specialist Group which advises the Forensic Science Regulator.

3. Most of my current income comes from instructions as an expert witness in complex digital evidence , for prosecution and defence in criminal matters, for claimants and defendants as well as single jointly in civil matters and for international criminal courts. My instructions have involved intercept, communications data and IP address evidence and have included terrorism, global hacking, paedophilia, narcotics trafficking, firearms offences, state corruption, murder, financial fraud, art fraud and money laundering.

4. Between 2003 and 2009 I was a member of the Scientific Advisory Panel on Emergency Response (SAPER) run by the Government's Chief Scientific Advisor, the remit of which included counter-terrorism and involved interaction with JTAC and others. . Since the withdrawal of the Draft Communications Data Bill in 2013 I have been providing, at their request, advice to Home Office officials.

5. The website www.pmsommer.com contains a full CV and pointers to relevant publications, submissions to Parliamentary Committees and legal instructions.

6. **What balance should be struck between the individual right to privacy and the collective right to security?** The issue is easier to resolve if recast in terms of types of intrusion, their justification in specific circumstances as a means of limiting harm, the arrangements by which the need for the intrusion is tested and authorised, how the intrusion is subsequently managed (including for collateral intrusion), and the extent to which each stage is auditable so that, after the event if not during, compliance failures can be detected and remedies made available. The difficulty with the ISC's consultation question, as framed, is that one may end up with little more than a very commonplace and abstract generalisation.

7. It is not enough, either, simply to look at broad classes of technologies; one must consider the many ways in which they can be deployed. As technologies of collection and analysis develop over time, issues of extent of intrusion change as well. It is possible to illustrate this by reference to the two technologies identified by the ISC:

8. **CCTV.** There are many different types and forms of deployment, for example:

Privately owned, Home Office Code of Practice - compliant[i]	Captures all passers-by. Only looks at public locations. Controlled by owner, released to Law Enforcement (LE) and Agencies on request or via Production Order. Has to be manually reviewed. Mostly used after the event, to identify perpetrators and their movements
Local Authority – crime prevention	Captures all passers-by. Only looks at public locations. Controlled by owner, released to LE and Agencies on request or via Production Order. Often viewed live. Has to be manually reviewed. Can detect events in commission but can also be used post-event.
Installed covertly as intrusive surveillance	Installed for specific need under RIPA s 32 – intrusive surveillance (and other Acts). If installed within property – under Police Act 1997 Part III (Authorised by SoS or Senior Authorising Officer) and s 5 ISA, 1994[ii]. Can detect events in commission but can also be used post-event.
Road Traffic + Automatic Number Plate Recognition	Captures all passers-by; 12m+ records per day [iii]. ANPR is captured digitally without manual intervention and stored for many years – provides detail on movements of vehicle and by inference, owners. Can be combined with other data in digital form

Future – facial recognition	Requires combination of high resolution cameras, ability to capture sequence of shots and ability to convert to 3D "face" plus database of suspects

9. **Communications data.** This term, from RIPA, 2000, also covers a number of different circumstances:

Fixed land-line calls – criminal investigation	Call Data Record – who called whom, when and for how long - acquired for all customers and stored by CSP[iv] for 12 months[v]; obtained by LE under RIPA s 22 – requires LE SDO to make judgement about necessity and proportionality
Mobile phones – criminal investigation	Call Data Record as above but also includes geolocation data. Geolocation data , acquired for all subscribers and stored by CSP for 12 months, for all times phone is powered up, not just when a call is being made - shows an individual's detailed movements for all this period. Cell Tower Dump – all phones powered up in a specific area – obtained by PACE Production Order
Web-browsing – criminal investigation	Top level – all website accesses by all subscribers but only up to first back-slash - acquired and stored by CSP for 12 months and obtained under RIPA (this is one area which the Communications Data Bill wanted to alter)
Email activity - criminal investigation	For all subscribers: who writes to whom but not content – 12 month storage by CSP, released under RIPA/Data Retention Directive
Intelligence Agency use of the above	Available under ISA, RIPA and s 94 Telecommunications Act, 1984 but also according to Snowden, by other means as well - acquired and stored by GCHQ – only controls are purely internal - Commissioner reliant on accuracy and completeness of GCHQ records

10. **Testing Intrusion Methods.** It is possible and more useful to identify a series of tests based on principles rather than the existing legislation. The starting point is that intrusion needs to be justified. Notions of individual privacy including

"correspondence" (which includes phone calls and emails) are deeply embedded in Western and international thinking – Art 12, UN Universal Declaration of Human Rights, 1948, Art 8, European Convention on Human Rights, 1950, and 4th Amendment to the US Constitution, 1789.

11. Looking first at ***effectiveness***: How far and in what ways does the specific intrusion method address the claimed harm?

    - Does the method help directly ***detect*** the harm in the first instance?
    - Is it a potential ***witness*** to harm that has not hitherto been detected?
    - Does it have a supporting role in ***post-incident investigation***?
    - Are statistics and supporting information available to support any claims around the above?[vi]
    - How does it mesh in with other methods of intelligence gathering, such as: open source, self-publicity by would-be perpetrators, alerts from the public and others, information gathered in the course of other investigations, suspicious activity such as the purchase of materiel and training, conventional physical surveillance, CHIS and information from financial institutions?

12. Looking specifically at the ***technological method***:

    - Does the method collect data globally from an entire population or only a small sub-section of which is likely to fall under suspicion?
    - Does the method inevitably collect more data / information from a suspect than is required for the investigation into the alleged harm?
    - What controls exist to limit access to / use of data which is not required or no longer required for the investigations?
    - How easy is it to combine the acquired data with other streams of data acquired by other methods so that the amalgamated intrusion is greater than the sum of its constituent parts?
    - What is the process by which authorisation to acquire / have access to takes place?
    - Where there is routine global non-targeted acquisition of data, is there a separation between the entity that collects that data and the agency that wishes to make use of it – such that on each occasion the requesting agency must justify their requests in terms of necessity and proportionality?
    - Does the intrusion mechanism and any associated controls have implications for trust in institutions in which society has a significant interest, such as the privacy of communications, the central operation of the Internet, and the use of encryption techniques for authentication of parties to a transaction and safeguarding citizens against eavesdropping to criminal purposes? These issues can have, among other things, profound economic implications[vii]. Is

there a mechanism, in government and in the oversight apparatus, to ask these questions?

- What policies and procedures exist to destroy data when there is no longer any justification for holding it?
- What audit schemes exist to detect / log usage *ultra vires*?
- What audit / oversight mechanisms exist to verify compliance?

13. Some, but not all, of these questions appear in the current Code of Practice for Covert Surveillance and Property Interference. [viii]
14. **Transforming and Combining Effects of Newer Technologies.** Changes which may appear, moment by moment, to be incremental, can nevertheless have a transforming effect. In relation to intelligence analysis: much more information is generated in digital form as a result of the use of computers, mobile phones and others; costs of collection fall all the time, costs of data storage fall all the time, costs of computer-aided analysis fall all the time. Costs of digital surveillance, compared with more conventional means, fall all the time. Once intelligence material is in computer-readable form it can be readily combined and aggregated[ix] so that while surveillance becomes "easier and cheaper", levels of effective intrusion increase as well. Geolocation data from mobile phones combined with ANPR from cctv combined with email communications data (which excludes content but identifies to whom an email was sent) combined with web-browsing activity (the web-site but not the individual page) enables the easy drawing of inferences and levels of intrusion which may not have been envisaged when the authorisations for each separate source were given.
15. The now-abandoned Draft Communications Bill made an initial (and rather unclear) attempt at managing combined sources of potential evidence in the "Request Filter"[x]
16. There is an argument which is sometimes advanced by the Agencies that, while they may hold quantities of data there is no intrusion unless it is accessed[xi]. The difficulty with this is that whereas in the purely criminal procedure communications data is held by the CSPs and only released to law enforcement after a proper, recorded procedure (s 22 RIPA), in the case of GCHQ, the process appears to be entirely internal. The Commissioners and the ISC are wholly dependent on there being a very reliable audit trail – and their ability to have sufficient technical knowledge to spot where there may be gaps.
17. The argument "we need the haystack to find the needle" [xii] should be tested for actual examples. It also assumes that the Agencies know what a specific "needle" looks like.
18. A further argument sometimes made by the Agencies is that there is no recorded evidence of abuse by them of communications data. This surely cannot be taken as definitive evidence that there has been no abuse. It is helpful to compare not dissimilar institutions, the police and the military, who have to make very difficult decisions rapidly and on imperfect information. Although these institutions, like

the Agencies, are basically ethical nevertheless significant cover-ups occur, for example, Hillsborough in the case of the police, Iraq breaches in the case of the military. Reasons include: to save careers and the desire to maintain "public trust" in the institution. In the case of the Agencies there would also be a perceived need to protect sources and methods. It is part of the stock-in-trade of the Agencies to conceal. It is also worth noting that more than 1,100 DWP staff have been warned over prying on benefits records[xiii] In addition, instances of mistakes by the Agencies in assessment abound[xiv].

19. The scenarios for longer-term concern, even if they could seem remote at the moment, but which any legal and oversight mechanism should anticipate are:
    - Arrogant rogue Agency employees who think they know better than the public and elected politicians[xv]
    - Politicians in difficulty and unable to distinguish party interests from national security and seeking to use information to discredit opponents and limit legitimate dissent

20. Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted. Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

21. It is difficult to provide detailed commentary and proposals within the ISC's requested 3000-word limit. I am happy to provide more detail on another occasion.

22. Law reform is relatively pointless unless one simultaneously considers means of enforcement. In most instances that implies the availability of admissible evidence. That, and the problems of open courts would create huge difficulties for the Agencies as it would reveal methods. Thus, a reformed law could only be part of a solution to re-assuring the public about Agency behaviour; it would also need to include credible, trustworthy and powerful oversight.

23. There also seems, with respect, relatively little point at looking at one set of methods of investigation / intrusion without considering the others, in particular those where technological change has transformed capabilities. The other important technologies are – referred to in NSA documents as Tailored Access Operations:

    - The use of audio and video bugs, the use of hardware to bug or otherwise compromise computers, phones and other devices. These come into the category of "interference with property". For regular policing activities these are addressed in Part III of the Police Act 1997 and for the Agencies under ISA 1994 ss 5-7. Access to a computer by an "enforcement officer"

which would otherwise be an unauthorised access for the purposes of s 1 Computer Misuse Act, 1990, (CMA) is protected under s 10 of the same Act.

- Intrusion into a computer using software, an offence under s 3 of the CMA and is not covered by the s10 exception, nor, I suspect, by ISA ss5-7.

24. Current surveillance legislation is spread over several laws and subject to a variety of authorisation regimes. RIPA covers intercept (authorised by Secretary of State), communications data (authorised by Senior Designated Officer - SDO), interference with property (bugs, taps) is authorised by Secretary of State (Agencies) and SDO (criminal – under Police Act 1997), CMA s10 allows LE access to computers in the course of their duty but does not cover if such access involves a s3 CMA offence, by using software backdoors – and ISA does not appear to give this power to the Agencies either. Physical seizure of computers under PACE requires a judicial warrant.

25. This confusion is difficult for law enforcement and only slightly less so for the Agencies. It is also difficult for politicians and other policy-makers to understand the range of powers. There thus seems a strong argument for a radical revision, similar to that involved in the Police and Criminal Evidence Act, introduced in the 1980s after dissatisfaction with the use of police powers under the old Judges' Rules.

26. My outline suggestions for law reform are thus:

- Research and produce a new integrated surveillance powers law with the emphasis on levels of intrusion, similar to the existing "Directed" and "Intrusive" models in ss 28 and 32, RIPA rather than based on specific technologies. Use Codes of Practice issued under SIs for the detail. The new law should cover intercept, communications data, bugs, taps and computer intrusions.

- Recognise that, because it is now all "data", the distinctions between intercept and communications data are difficult to realise in practice (try applying them to a Facebook page or mobile phone app) so that the issue here too is level of intrusion. Remove the existing inadmissibility rule on intercept[xvi].

- Consider, as an alternative to whole-population data retention, targeted Data Preservation Orders requiring CSPs to collect and hold data (intercept and comms) of identified persons against the time at which a full warrant is authorised.

- While maintaining the role of Secretary of State for authorising Agency strategy and broad operations, place the granting of individual warrants with judges[xvii]. This would be more in line with international practice,

provide a "separation of powers" and enable judges to build expertise in surveillance technologies in a way no Minister would ever have time. The argument about Ministerial democratic accountability to Parliament collapses when one accepts they will never discuss operations and methods in public and can thus never be challenged.

- Limit Law Enforcement and Agency powers of self-authorisation to the very lowest levels of intrusion.
- Build into legislation, including ISA, and related Codes of Practice the need for the maintenance of full audit records
- Add to the ISC remit a specific requirement to consider the impact of Agency activity on society as a whole[xviii]
- Develop a robust route for Agency whistle-blowers

27. **Oversight Mechanisms** The ISC's Call does not refer to the effectiveness of oversight but, given the problems of testing surveillance law compliance in open court, trust in the quality and depth of oversight becomes crucial. I note that the ISC has yet to publish its Memorandum of Understanding[xix]. Both the Commissioners and the ISC must acquire resources enabling them to identify and pose questions covering technical surveillance capabilities and how they are deployed.

I would be happy to enlarge on any of these matters.

20 January 2014

---

[i] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

[ii] Also see Code of Practice: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf

[iii] http://www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf

[iv] CSP: Communications Service Provider – incorporates Telephone companies, mobile phone companies and Internet Service Providers

[v] Data Retention (EC Directive) Regulations 2009; http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents

[vi] See http://www.washingtontimes.com/news/2013/oct/2/nsa-chief-figures-foiled-terror-plots-misleading/?page=all#pagebreak; http://politicalscience.osu.edu/faculty/jmueller/NSAshane3.pdf, http://newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1.pdf

[vii] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10431825/Inventor-of-world-wide-web-criticises-NSA-over-privacy-breaches.html, http://www.bbc.co.uk/news/technology-25033577, http://www.scmagazineuk.com/nsa-backlash-continues-uk-firms-move-data-out-the-us/article/329224/?DCMP=EMC-SCUK_Newswire

[viii] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf

[ix] According to Snowden, the main NSA resource is XKeyscore (http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data) but commercial programs used by law enforcement also provide similar facilities, if on a smaller scale, eg Nuix (http://www.nuix.com/Investigation) and I2 Analysts' Notebook (http://www-03.ibm.com/software/products/en/analysts-notebook/)

[x] Clauses 14-16, Draft Communications Data Bill, http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf

[xi] David Omand: http://www.theguardian.com/commentisfree/2013/jun/11/make-surveillance-ethical-and-effective

[xii] Iain Lobban in oral ISC evidence, 07/11/2013

[xiii] http://www.telegraph.co.uk/news/10561388/More-than-1100-DWP-staff-warned-over-prying-on-benefits-records.html

[xiv] See, for example, *UK Eyes Alpha*, Mark Urban, *Empire of Secrets*, Calder Walton, *GCHQ*, Richard J Aldrich. Perhaps one can add the examples of Adebowlae and Adebowale, known to the authorities but not tracked. See http://www.independent.co.uk/news/uk/crime/theresa-may-keen-to-revive-snoopers-charter-in-wake-of-woolwich-attack-8629990.html

[xv] *UK Eyes Alpha*, ibid

[xvi] S 17 RIPA

[xvii] There would be a graduated scheme depending on levels of intrusion

[xviii] In ISA s10 and J&SA 2013, Part 1 s 2

[xix] S 2(5-6) J&SA