Submission to the Intelligence & Security Committee by Peter John MEng MBCS, February 2014

System Administrator NoDPI.org (an online communications forum), Author of Dephormation and Secret Agent (surveillance countermeasures)

Contact Details:

[REDACTED]

About me:

I'm a British software engineer, with approximately 25 years experience in the UK IT/Telecommunications industry. Now a UK ex pat, living in Europe.

I played a prominent role in the campaign against the BT/Phorm scandal. In March 2009 I organised the meeting at the House of Lords attended by Sir Tim Berners Lee and Dame Wendy Hall, at which the topic of Phorm's surveillance technology was discussed.

I am the administrator of the NoDPI (no deep packet inspection) campaign site, and the author of the Dephormation & Secret Agent counter-surveillance tools.

Executive Summary:

This submission compares the nature & regulation of the internet with earlier telegraph networks, reviews the present threat to the United Kingdom from terrorism & crime, provides personal insights into the enforcement (or otherwise) of the Regulation of Investigatory Powers Act, and makes a strong case for the following recommended changes to regulation of UK telecommunications;

I. **An explicit and specific warrant for every intercept**; on the basis that the UK is a democratic nation of innocent people with a right to private communication under the ECHR. The police serve the public. The public do not serve the police.

II. Reform the oversight & enforcement regime, to **separate those people responsible for enforcing the law governing interception of communications** from the **criminals who are responsible for breaking the law**. Currently, this is emphatically <u>not</u> the case.

III. **Increase the current penalty for unlawful interception** from £50,000 **to an unlimited fine with a mandatory ten year prison sentence.** Personal experience suggests that the police & regulators will cite the trivial nature of penalties as a reason to deny law enforcement.

IV. **Remove all oversight functions from corrupt politicians who are incapable of protecting & serving their constituents effectively,** and **put it in the hands of the**

public (particularly people with significant technology and/or human rights protection experience and demonstrable independence).

V. **Immediately remove Ian Livingston from his post in the House of Lords and Government.** Lord Livingston was the BT CEO who oversaw the events of the BT/Phorm affair, and was primarily responsible for unlawfully divulging some or all of the content of UK telecommunications to foreign spyware criminals, without warrant or consent, in 2006/7/8. **Ian Livingston is a traitor, a recidivist criminal, and a spy.**[1]

VI. **Remove Nick Gargan from his post as Chief Constable of Avon & Somerset police**, and replace him with a senior officer who recognises that unwarranted covert interception of UK telecommunications is a criminal offence. A criminal offence that the police are – unequivocally - responsible for investigating and prosecuting.

VII. **Dismiss the treacherous senior management of GCHQ**, for covertly and illegally divulging en mass the content of private/confidential UK telecommunications to foreign Governments, so facilitating damaging political & economic espionage.

Introduction:

The committee's consultation is the latest in a series of repetitive consultations concerning mass surveillance, all covering broadly similar topics.

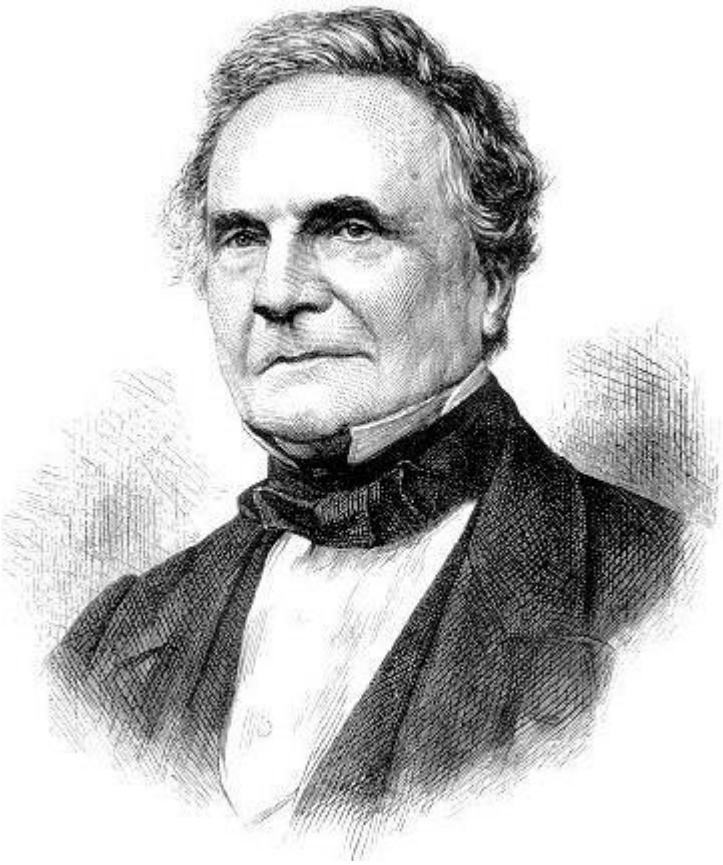
Other examples include the consultation by the Joint Committee on the Draft Communications Data Bill (in 2012), the Home Office consultation "RIPA: proposed amendments affecting lawful interception" (2011), and the APComms consultation that preceded the report "Can we keep our hands off the net?" (2009)... and others.

With the benefit of hindsight and the revelations of the Snowden disclosures, it is quite obvious that those time-wasting and fatuous exercises in faux 'consultation' were based on a completely false premise maintained by the Home Office and UK security services... that the communications data gathered by UK intelligence services was constrained by warrants, strictly governed by laws, and monitored closely by regulators.

I'm disappointed to note that you have chosen to present the current consultation using services hosted by Google in the USA (rather than a UK service provider), and invited submissions using a proprietary document format devised by Microsoft (a US software provider). It seems to me that you have learned nothing from the revelations published by the Guardian and other newspapers concerning US methods of surveillance. Or perhaps I misunderstand your motivations in so doing?

[1] https://www.whatdotheyknow.com/request/appointment_of_ian_livingston_ii

> On two occasions I have been asked [by members of Parliament], 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question.



Response:

a) What balance should be struck between the individual right to privacy and the collective right to security?

How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras? To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security? How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?

To dispel those myths that evidently underpin your question...

Myth: 'The Internet is New and Revolutionary'

1. There is no significant difference, in principle of operation, between internet communications and generations of earlier data communications technology. Even the use of optics in telecommunications can be traced back to the Heliograph[2] (in the 1820s) or Photophone[3] (in 1800), long before the advent of lasers & fibre optics used by the modern internet.
2. Speed and costs have varied, methods of transmission and protocols have changed, volumes of data have increased, but the internet is & remains a global telegraphy network at its core. Everything you see today is not a 'revolution', it has evolved gradually from the legacy of the global telegraph network[4].
3. In 1880 Henry Fawcett, answering concerns about unlawful interception of communications told Parliament; "I can assure my hon. Friend that any persons in the employment of the Post Office giving any information as to the persons sending telegrams, the persons to whom they are sent, or the contents of such telegrams, would not only be dismissed from the public service, but would, by **Section 20 of the Telegraph Act of 1867**, render themselves liable to prosecution".
4. The essential requirement for privacy of communications that existed in 1867 is no different today. However, commercial and political pressure to exploit this data and so weaken the rights of UK citizens to communicate privately has intensified.
5. **Unlawful communication surveillance results in the following examples of damage...**
    a. **Loss of personal liberty (freedom of speech, freedom of association, freedom of expression etc)**
    b. **Collapse in confidence in the privacy/security/integrity of the telecommunication network, resulting in greater use of encryption, or decreased use of public telecoms**
    c. **Economic damage to businesses that use unencrypted communications**

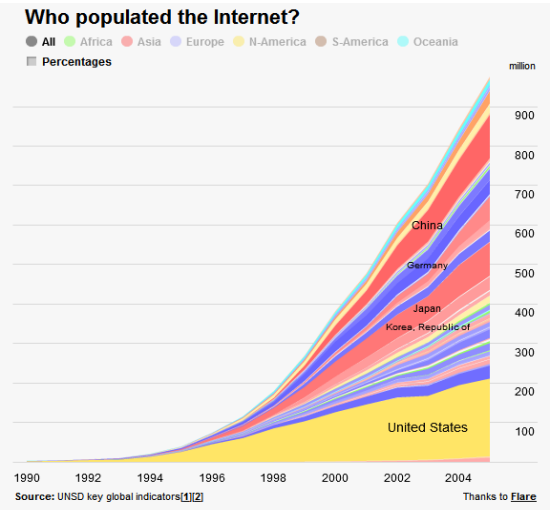
[2] https://en.wikipedia.org/wiki/Heliograph
[3] https://en.wikipedia.org/wiki/Photophone
[4] See "The Victorian Internet" by Tom Standage, ISBN-13: 978-0753807033

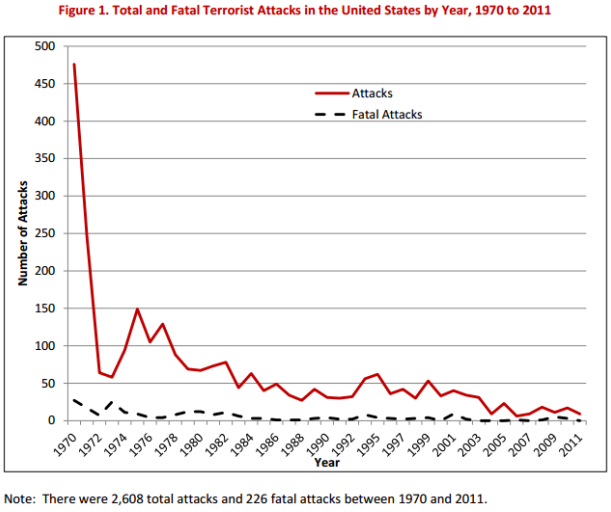
d. Increased cost of business associated with encryption

6. It is and always will be essential - to prolong the liberty & economic well being of UK citizens - that the privacy, security & integrity of the UK telecommunications network is protected against illegal spying.
7. Internationally, it is in the national interest to defend the UK telecommunications network from foreign surveillance (and for the avoidance of any doubt that would include industrial and political espionage by the USA).
8. Anticipating technological change, RIPA was intended to be 'technology neutral'.

Myth: 'The Internet is Breeding Global Terrrrrrrorists'

9. There is a popular misconception among UK (and American) politicians that the rise of the internet can be associated with a corresponding rise in international terrorism. Some interesting data published in recent years would appear to refute that assertion entirely.
10. The chart on the left below (source UN[5]) shows the rise of the Internet as a communications network. The chart on the right shows attacks & fatal attacks by terrorists in the USA spanning the same time period (source Washington Post[6]).
11. You will note, as global access to internet communications technology increases, the number of attacks by terrorists in the USA declines markedly.





12. In fact, if I overlay the two diagrams above (aligning the date axis) I get this picture;-

[5] http://data.un.org/Host.aspx?Content=Tools

[6] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/09/11/nine-facts-about-terrorism-in-the-united-states-since-911/

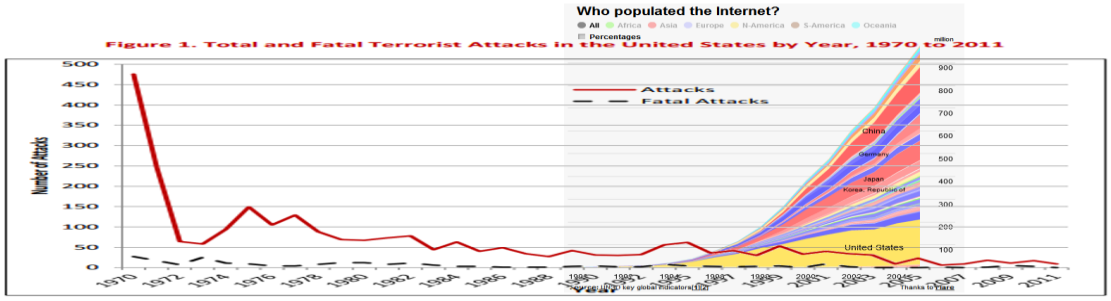


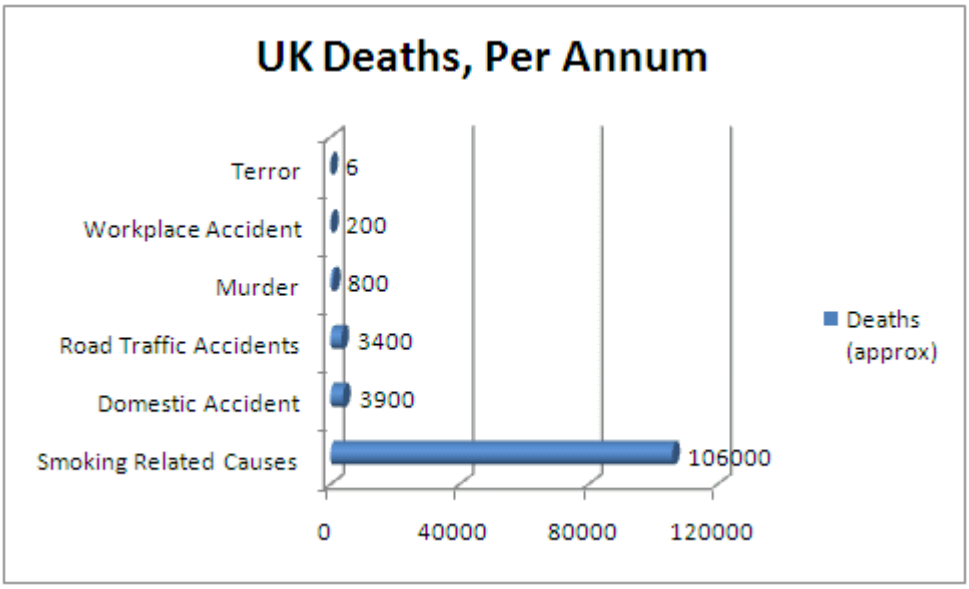
Figure 1. Total and Fatal Terrorist Attacks in the United States by Year, 1970 to 2011

Note: There were 2,608 total attacks and 226 fatal attacks between 1970 and 2011.

13. Which suggests one novel solution to global terrorism might be improving the availability & quality of trustworthy communications services, rather than systematically compromising & undermining them.

Myth: 'The UK Faces an Existential and Growing Threat from Terror & Crime'

14. It is important to understand that crimes like terrorism – often used by the Home Office to justify mass surveillance and data retention – presently pose a negligible risk to life in the UK;



15. To put those numbers in perspective, 6 people die every year falling out of trees. But there is no expectation that crash mats will be placed under all trees in the UK 'just in case'.
16. If you want to save lives, the conclusion is inescapable… better value can be derived by spending £billions preventing people smoking. Rather than spending £billions intercepting the communications of **innocent people** and the **law abiding businesses that serve them**.
17. The other crime frequently cited as justification for mass surveillance is the heinous offence of child murder/paedophilia. The Home Office (in the Communications Data consultation) cited the shocking examples of Ian Huntley & Levi Bellfield.
18. In the case of Huntley, however, it was revealed that he had been a suspect in a series of sexual offences and burglaries... yet had still been allowed to work in a school. **There is nothing to suggest that retention of public communications data would have prevented Huntley's offences. There was a serious failure by public**

authorities to accurately vet his background, and a serious failure by police to reconcile data on his behaviour.

19. Bellfield was named by police as a suspect in connection with numerous unsolved murders and attacks on women dating back to 1990, and the murder of a 14-year-old girl in 1980. Assistant Chief Constable Jerry Kirkby said, "Questions will be asked whether Bellfield could have been caught and we must accept, and do, that mistakes were made". **There is no evidence to suggest that retained communications data would have prevented Bellfield's offences.**
20. In both cases, a serious failure by police to correlate **available conventional intelligence** allowed the offences to occur.
21. The Office of National Statistics/Home Office announced in October last year that UK crime rates have reached an all-time low. It seems obvious that you cannot justify *increasing* surveillance while recorded crime is actually *falling* to *record lows*[7].

Proportionality and the ECHR

22. In terms of proportionality, please can I draw your attention to Article 8 of the European Convention on Human Rights (to which the UK is committed);-

> **Article 8 – Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

23. Retaining communications data of innocent people (and we are presumed innocent until proven guilty of a crime) is not proportionate to the threats we face. Unless you consider the UK a nation of criminal suspects.
24. The UK Government is presently subject to an ECHR complaint by the Open Rights Group (ORG) because the surveillance methods employed by GCHQ/NSA are not in accordance with the law, or proportionate to their claimed security purpose[8]. I support the ORG action, and sincerely hope they prevail.

b) 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.

[7] www.theguardian.com/uk-news/2013/oct/17/crime-figures-fall-record-low
[8] http://www.wired.co.uk/news/archive/2013-10/04/campaign-groups-take-british-government-to-court

25. The evidence of the Snowden revelations demonstrates clearly that there is a serious systemic problem of illegal and disproportionate communications surveillance.
26. However I believe **the most significant problem is complacent enforcement** & **oversight,** a resulting failure of compliance, and **not inadequate legislation.**

c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

27. **The unlawful interception of communications is already a criminal offence.** But few people are ever prosecuted. Particularly so police and security services staff.
28. In 2008 I was among those who reported BT & Phorm Directors to the police alleging various offences including illegal interception of telecommunications, as well as concomitant fraud, computer misuse, and commercial copyright theft.
29. In 2006/2007 BT/Phorm had covertly intercepted the private/confidential communications of hundreds of thousands of UK citizens, and the businesses that served them. Yet there were no arrests, no prosecutions, no penalties imposed.
30. The ICO refused to intervene. Ofcom claimed it had no powers to act. The various Surveillance Commissioners claimed they had no role to play. The police refused to investigate. The CPS refused to prosecute ... leading the UK Government to face the European Court of Justice[9].
31. The resulting **Regulation of Investigatory Powers (Monetary Penalty Notice and Consents for Interceptions) Regulations** were claimed to impose a penalty on any person who "has without lawful authority intercepted, at any place in the United Kingdom, any communication in the course of its transmission by means of a public telecommunications system and was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception concerned".
32. Yet subsequent similar examples of unlawful mass surveillance suggest the problem was never lack of legislation... but simply a complete enforcement vacuum.
33. In 2009 I approached Avon & Somerset police again to complain about unlawful mass surveillance, after I captured evidence that Vodafone UK were conspiring with an American company called Bluecoat. Vodafone customers' private communications data was being covertly intercepted and divulged to a third party in California for a replay attack, without warrant or consent from either party[10]. Despite unlawful interception & computer misuse, the police simply refused to investigate.
34. Likewise the Google Streetview affair, wherein UK wireless telecommunications were unlawfully intercepted and stored on Google's Streetview cars without warrant or consent from either party. Again, I complained about unlawful interception to Avon & Somerset police and again they refused to investigate.
35. The Home Office recently confirmed that if a complainant "believes that an offense has been committed, he should report this to the police"[11]. In my experience, reporting illegal interception to Avon & Somerset police is completely futile.

[9] http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html

[10] https://nodpi.org/2011/06/22/vodastalk-vodafone-and-bluecoat-stalking-subscribers/

[11] https://nodpi.org/forum/index.php/topic,6062.msg53332.html#msg53332

36. Since the **Regulation of Investigatory Powers (Monetary Penalty Notice and Consents for Interceptions) Regulations** was passed, there has been no greater willingness on the part of the police and regulators to enforce the law.
37. When I challenged Nick Gargan (Chief Constable of Avon & Somerset Police) to explain why his force refused to investigate each & every complaint I have made about unlawful communications surveillance, I was told (after he had finished laughing in my face) that intercepting communications and divulging some or all of the content to a third party without consent or a warrant was "not a crime" (in his words). [12]
38. That conversation - coming after five years of lies & obstruction over illegal surveillance by a fraternity of corrupt policemen, regulators, businessmen, and politicians - is at least one of the reasons why I decided to leave the UK.

Recommendations

39. I believe the following policy recommendations would demonstrate a new commitment to protect the privacy & security of UK telecommunications;-

I. **An explicit and specific warrant for every intercept**; on the basis that the UK is a democratic nation of innocent people with a right to private communication under the ECHR. The police serve the public. The public do not serve the police.

II. Reform the oversight & enforcement regime, to **separate those people responsible for enforcing the law governing interception of communications** from the **criminals who are responsible for breaking the law**. Currently, this is emphatically <u>not</u> the case.

III. **Increase the current penalty for unlawful interception** from £50,000 **to an unlimited fine with a mandatory ten year prison sentence.** Personal experience suggests that the police & regulators will cite the trivial nature of penalties as a reason to deny law enforcement.

IV. **Remove all oversight functions from corrupt politicians who are incapable of protecting & serving their constituents effectively,** and **put it in the hands of the public** (particularly people with significant technology and/or human rights protection experience and demonstrable independence).

V. **Immediately remove Ian Livingston from his post in the House of Lords and Government.** Lord Livingston was the BT CEO who oversaw the events of the BT/Phorm affair, and was primarily responsible for unlawfully divulging some or all of the content of UK telecommunications to foreign spyware criminals, without warrant or consent, in 2006/7/8. **Ian Livingston is a <u>traitor</u>, a recidivist <u>criminal</u>, and a <u>spy</u>.**[13]

VI. **Remove Nick Gargan from his post as Chief Constable of Avon & Somerset police**, and replace him with a senior officer who recognises that unwarranted covert

[12] See https://nodpi.org/2013/11/27/one-last-protest-avon-and-somerset-pcc-police-public-forum/
[13] https://www.whatdotheyknow.com/request/appointment_of_ian_livingston_ii

interception of UK telecommunications is a criminal offence. A criminal offence that the police are – unequivocally - responsible for investigating and prosecuting.

VII. **Dismiss the treacherous senior management of GCHQ**, for covertly and illegally divulging en mass the content of private/confidential UK telecommunications to foreign Governments, so facilitating damaging political & economic espionage.