To the members of the Committee,

Thank you for the opportunity to make a submission to your inquiry into privacy and security.

My name is Ray Corrigan. I'm a Senior Lecturer in the Maths, Computing & Technology Faculty of The Open University though I write to you in a personal capacity.

Executive Summary

Privacy and security are not opposites but mutually dependent. It is essential the committee understand that the false privacy v security dichotomy that so often frames public debate seriously undermines policymakers' and the public's understanding of the issues at hand. The single most important airline security measure put in place following the terrible attacks on September 11th 2001 was the reinforcement of cockpit doors. That had absolutely no impact on the personal privacy of travellers. The hugely expensive naked scanners installed at airports, however, take a terrible toll on personal privacy whilst being functionally worse than useless as a security measure (and the X-ray variety has been shown to pose a risk to health). A door lock or a strong high fence provides security without compromising privacy.

Massive data collection and mining compromise privacy and security. The NSA gave 850,000 people access to classified materials as a routine part of their jobs. Their systems are big and complex and require a lot of staff to operate but there can be no security when that number of people has access to secrets.

There is no "balance" to be achieved between the "individual right to privacy and the collective right to security". The collective right to security requires an individual and collective right to privacy. The value of protecting individual and collective privacy is that those rights make a fundamental contribution to the overall health of society. Framing privacy as the opposite of security assumes privacy is only about hiding bad things. That couldn't be more wrong.

It is fundamentally incompatible with the rule of law to collect information about every member of the population in the hope of conducting post hoc fishing expeditions to look for evidence of misbehaviour. Could I remind the committee of the belief of Cardinal Richelieu that given 6 lines written by the most honest man he could show you the evidence to hang him.

It is unnecessary and completely disproportionate, not to mention dangerously ineffective, "to collect innocent communications in order to find those who might threaten our security." Finding a terrorist or serious criminal is a needle in a haystack problem – you can't find the needle by throwing infinitely more needle-less electronic hay on the stack. Law enforcement, intelligence and security services have to be able to move with the times. They need to use modern digital technologies intelligently in their work and through *targeted data preservation regimes* – not the mass surveillance regime they are currently operating – engage in technological surveillance of individuals about whom they have reasonable cause to harbour suspicion. That is not, however, the same as building an infrastructure of mass surveillance which, incidentally, in addition to being a clear and present danger to democracy, makes it *mathematically impossible* for dedicated intelligence services staff to do their job with any degree of effectiveness.

The committee should understand that computers are not magic. These machines do exactly *what they are programmed to do* not *what you would like them to do*. I make this point specifically in light of the Prime Minister's recent comments to the effect that the TV crime drama he likes so much justifies the mass data collection activities of the intelligence services. TV crime drama and

Hollywood films generally are *terrible* guides to how computers actually work in practice. The committee should additionally understand that there is no clear distinction to be made between communications data (or so called meta data) and communications content. If it is difficult to define the distinction from a social or legal perspective it is impossible to implement from the technical perspective.

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)?

If the committee only takes one thing away from this submission let it be this –

- Privacy and security are ***not*** opposites.

- There is *no* balance to be struck between the individual right to privacy and the collective right to security.

Privacy has an image problem. It is constantly portrayed as out of date, costly, an obstacle to public safety and new and exciting forms of commerce and research. So if we pitch privacy against something as essential as national security, it is a no contest. What does it matter if we have to dispense with a little personal privacy for the guaranteed gain of being safer and more secure?

It matters because when you start with this fundamentally flawed premise and the committee's flawed question, it leads you to the wrong answers. The notion that privacy has to be sacrificed for security is wrong. More privacy does not mean less security any more than more security means less privacy. The associated (unspoken) idea that individual privacy is damaging to society is wrong. There's no strict division between individuals and society. The welfare of both is inextricably interlinked. The fundamental right to privacy of the individual is one of the foundation stones of a healthy society. The value of protecting individual and collective privacy is incalculably important to the future of our information society.

The constant refrain about the need to balance privacy and security is quite simply wrong because it has a number of built in assumptions that are wrong.

It assumes that privacy and security are opposites which is false. A locked door and a tall strong fence provide security and facilitate privacy. A reinforced cockpit door – the most important airline security measure put in place since the atrocities of September 11th 2001 – does nothing to compromise privacy.

It assumes that undermining privacy through the use of magic modern computer systems will improve security. This is false. Democracy and freedom requires privacy and security. That such mass surveillance will not work can be demonstrated mathematically.

The esteemed chairman of the ISC, Mr Rifkind, has stated in parliament (in the debate on oversight of intelligence & security services on 31st October 2013) that

> "Of the totality processed by computers, perhaps 0.01% will have selectors that the computer has been programmed to look for. The communications of the other 99.99%—covering virtually every citizen of this country, bar a very small number—are never even looked at by the computer, other than in relation to a selector, such as an e-mail address. Even for the tiny minority identified by the computers as potentially relevant to terrorism, if GCHQ, MI5 or MI6 want to read the content of any of the e-mails, they have to go to the Secretary of State for permission. Under the law, only if they are given permission can the content be read"

I'm going to do some very rough maths here in an attempt to explain the problem with Mr Rifkind's point that only 0.01% of communications data is looked at.

0.01% of 60 million people in the UK implicates 6000. Now the pattern flagging will be nowhere near as simple as that but just run with it as a crude estimate. We know from the deputy director of the NSA testifying before the House Judiciary Committee that you don't need to be a terrorist or have contact (deliberate or inadvertent) with a terrorist to be flagged as suspicious. The NSA (and presumably GCHQ?) is allowed to travel "three hops" from its targets – who could be people connected to people connected to people connected to you. 0.01% of the UK population or 6000 people are 2 degrees of separation from about 160,197,360 and 3 degrees of separation from over *26 billion* others (about three and a half times the population of the world).

Even limiting suspicion to two hops, your 0.01% of data on UK residents, Mr Rifkind, implicates more than 2.6 times the entire UK population. So the question then becomes, given that we are all suspects, who decides which suspects the intelligence services' limited resources should be deployed to further investigate and pursue, once the computer algorithms have worked their magic?

Every time the (theoretically 99.99% effective) magic terrorist catching system is asked for a suspect it implicates vastly more people than the security services could possibly investigate in any detail.

Mr Rifkind also rightly stated "Modern computers... are programmed to run using certain selectors". So who gets to program the computers and what are the specific 'selectors'/filters? Who decides what the selectors should be? Who decides who decides what the selectors should be? The chair of the ISC doesn't understand computers, so how can he effectively and his committee scrutinise the technical aspects of this work? How do you measure the efficacy of these filters given it is widely known in the tech community how ineffective electronic filters can be? How, when someone is tagged as suspicious via these secret algorithms, does the information on that individual then get further processed? What happens when someone is wrongly tagged and how do they retrieve their innocence and clean bill of electronic health? Are you aware of the nature of false negative results and false positive results?

In multiple media engagements the Prime Minister, the Home Secretary and other members of the government refer to "protecting the public" from the four horsemen of the infocalypse - terrorists, drug dealers, child abusers and organised crime - and more. The Prime Minister last week extolled the virtues of TV crime dramas as a guide to how electronic surveillance systems should be deployed in practice. TV crime drama and Hollywood films generally are *terrible* guides to how computers actually work in practice.

Mathematically the four horsemen are not problems that lend themselves to mass data mining. Even highly accurate (to 99.99% and by the way no current system comes close to that) data mining systems will swamp investigators with false positives when dealing with a large population. Law

enforcement authorities end up investigating and alienating large numbers of innocent people. That's no good for the innocents, for the investigators or for society.

There is an oft repeated the myth that the 9/11 attacks would have been prevented if only the US intelligence and security services had known where Mohamed Atta was when he had made a phone call to a terrorist suspect in Syria. The assumption is the magic terrorist catching mass data collection and analysis apparatus now run by the NSA would have pinpointed his location and led to his arrest.

Wrong.

Atta was known to the intelligence and security services and considered a threat. Police, intelligence and security systems are imperfect. Even in 2001 they processed vast amounts of imperfect intelligence information. At least one FBI agent believed Atta to pose a serious and imminent threat. That belief got lost in the noise of the intelligence information processes, suspects and issues the agencies were then dealing with, to the degree that they did not detain Atta or his associates and prevent the attack.

There was too much data noise in the system and they lost him. You **cannot** cure that excess of data noise problem by treating the entire population as suspects, engaging in suspicionless, blanket collection and processing of personal data. You **cannot** find the real terrorist by assuming everyone is a threat.

Mass data collectors can dig deeply into the digital persona of *anyone* but don't have the resources to do so with *everyone*. The resultant pursuit of false positive leads mean the real bad guys often get lost in the noise, as happened with the 9/11 attackers including Atta who were known to US authorities but not considered sufficiently important to intercept.

Finding the four horsemen is a needle in a haystack problem and you can't find the needle by throwing infinitely more needle-free hay on your stack and/or creating multiple giant and exponentially growing data haystacks.

Operating multiple massive databases of intimate personal communications data makes the public more vulnerable to the four horsemen not less so.

That such mass databases are useless for finding terrorists is clear from the maths and the evidence. The NSA has admitted in spite of previous claims that their mass data collection and analysis stopped 54 major terror attacks since 9/11 it didn't really stop any, but may possibly have provided secondary supportive evidence in relation to one. The most recent argument they used to support the deployment of such systems is mass data collection might be useful as an "insurance policy". An insurance policy?! The infrastructure of mass surveillance might be useful in the future, somehow, to someone?

That such systems also make the public less safe is associated with the impossibility of securing mass silos of valuable personal data. Computer scientists simply do not know how to keep databases of the magnitude of those used by the NSA and GCHQ secure from external hackers or the multitude of insiders who have access to these databases as a routine part of their jobs (850,000 including Edward Snowden in the case of the NSA). Security experts like Ross Anderson, Bruce Schneier, Edward Felten and Peter Sommer have written extensively about this. To understand this you have to think about how such systems can fail - how they fail naturally, through technical problems and errors (a universal problem with computers), and how they can be made to fail by attackers (insiders

and outsiders) with malign intentions e.g. the four horsemen. When the inevitable hacks, leaks, data contaminations happen, what then?

In its most insidious form the misleading privacy v security question is phrased as a statement along the lines "the innocent have nothing to hide". This assumes two underlying falsehoods – firstly that privacy is only about hiding bad things and secondly that decimating privacy will solve the problem du jour. I hope I've demonstrated clearly to the committee that both these assumptions are wrong and that in answer to your questions –

- There is no balance to be struck between the individual right to privacy and the collective right to security
- It is neither necessary nor proportionate nor effective to engage in blanket monitoring or collection of innocent communications in an attempt to find those who might threaten our security

On the question of whether the intrusion differs between data and content I would refer you to Peter Sommer's writings and analysis e.g. analysis at
http://scramblingforsafety.org/2012/sf2012_sommer_commsdata_content.pdf
And his evidence before the select committee on the Communications Data Bill.

> *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.*

The notion that the day to day activity of every citizen should be recorded in the expectation that those records can, in future, be mined for nefarious activity is anathema to a healthy functioning liberal democracy. Yochai Benkler in a recent Guardian article (http://www.theguardian.com/commentisfree/2013/oct/16/nsa-fbi-endrun-weak-oversight) put it more eloquently than I could:

> "Mass surveillance represents a commitment to near-universal all-seeing gaze, so as to assess and respond to threats that can arise anywhere, at any time. Privacy as a check on government power represents a constitutional judgment that a limited government must have limited power to inspect our daily lives, and that an omniscient government is too powerful for mere rules to restrain. The experience of the past decade confirms this incompatibility...
>
> Technology has enabled government to have investigative and situational awareness on a scale and scope that were science fiction when the Stasi shut its doors. The "state of emergency" mindset necessary to justify the program in the first place drives those charged with assuring the safety of Americans to always use this technology to its full potential; it also gives them an independent source of legitimacy for their actions – the fierce urgency of necessity.
>
> Their mission clashes with the fundamental premise of privacy as a civil right: that state power is best contained by making the overwhelming majority of what goes on in society invisible to the state. As Justice Alito put it in the supreme court's decision to strike down GPS tracking:
>
> [Historically] the greatest protections of privacy were neither constitutional nor statutory, but practical.
>
> Once the state knows about behaviour, it is hard to rely on rules alone to bear the full burden of preventing overreach by those who wield its awesome power...

Rules alone cannot hold back the millions of potential abuses of an omniscient state.

As long as government is allowed to collect all internet data, the perceived exigency will drive honest civil servants to reach more broadly and deeply into our networked lives."

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

As Jemina Stafford QC made clear in a formal opinion for a parliamentary committee last week, (http://www.tom-watson.co.uk/wp-content/uploads/2014/01/APPG-Final.pdf) the current mass data collection activities of sections of the UK government already undermine the right to privacy guaranteed in the Human Rights Act and article 8 of the European Convention on Human Rights. It is clear that the Regulation of Investigatory Powers Act does require an update but I don't have any specific proposals to put before the committee at this stage.

However, I do have a general proposal that *suspicion should be the test for surveillance*.

The government of course has the right to intercept and record information when someone is suspected of a serious crime. But current operation appear to involve collection of data without suspicion: which is in effect mass surveillance. Due process, since the 1765 case of Entick v Carrington, requires that surveillance of a real suspected criminal be based on much more than general, loose, and vague allegations, or on suspicion, surmise, or vague guesses. To operate the mass date collection and analysis systems GCHQ has been reported as doing which give the entire population less protection than a hitherto genuine suspected criminal, based on a standard of reasonable suspicion, is indefensible. The gathering of mass data to facilitate future unspecified fishing expeditions is indefensible in law.

I appreciate the ISC and a multitude of highly dedicated public officials are grappling with really complex issues here. But it is critically important that you understand –

- Privacy and security are ***not*** opposites.
- There is *no* balance to be struck between the individual right to privacy and the collective right to security.
- Computers are not magic and never will be
- Mass data collection and analysis is mathematically provable to be unfit for the purpose of hunting the four horsemen of the infocalypse

It is also hugely important that you be provided with the resources and expertise required to fulfil the immensely demanding duties required of the committee.

I'd leave you with one final thought. Nearly 250 years ago, Lord Chief Justice Camden decided that government agents are not allowed to break your door down and ransack your house and papers in an effort to find some evidence to incriminate you (the case of Entick v Carrington (1765) 19 Howell's State Trials 1029, 2 Wils 275, 95 ER 807, Court of Common Pleas).

The good judge also declared personal papers to be one's "dearest property". I suspect he might view personal data likewise in the internet age. I understand Lord Camden's reasoning in Entick became the inspiration behind the 4th Amendment to the US Constitution which offers protection from unreasonable searches and seizures. For a quarter of a millennium, fishing expeditions of the type that the GCHQ and NSA are engaged in have been considered to fundamentally undermine the rule of law. It's time Parliament brought these modern practices into line with that rule of law.