Rt. Hon. Sir Malcolm Rifkind MP,PC,QC .
Chairman
The Intelligence and Security Committee of Parliament
35 Great Smith Street
London SW1P 3BQ

4th Feb 2014.

Dear Sir Malcolm,

I would like to thank you for your kind invitation of 19th Dec 2013 to submit evidence to your inquiry into privacy and security.

My locus for responding is unusual but I hope helpful.

Brief background

I am a former army infantry officer with direct experience of terrorism. I am a full professional Fellow of the British Computer Society (FBCS.CITP) and a systems analyst. Between 1984 and 1988, I was the House of Commons researcher for (Rt.Hon.Lord) Paddy Ashdown - a former Royal Marine Captain, and later an M16 station head (see his autobiography) dealing with a related issue to that raised by the Committee. I am the author of Trade Wars (1986), which dealt with illegal trade conduct in the UK in violation of UK sovereignty. More recently I sponsored a lecture in Committee Room G of the House of Lords on 18th April 2012, given by (the late) Professor Dr Hans Meuer, the father of European supercomputing (Attached). I am the author of the Computer Weekly guide to supercomputing 2012 (Attached). Supercomputers are the primary tool in all modern intelligence work.

I write books about landownership (*Who Owns Britain and Ireland* and *Who Owns the World*) and I am a journalist.

Before embarking on the issues raised by the Committee, I would like to make an observation.

The issues the committee raises are without a context. The implied context is 'privacy' and 'security' but neither word is defined or explained. Neither are the structures, legal or otherwise, affecting privacy and security set out or explained. There are upwards of 14 statutes covering the issues of security and of privacy in one way or another.

Yours sincerely

Kevin Cahill

Kevin Cahill FRSA, FRGS, FBCS.CITP, FRHistS, BA
1 Kingfisher Drive, Exeter, EX4 4SN
Mobile 07787176706
E-mail. Ros@globalnet.co.uk

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Index

Appendices

Brief history of American illegalities in the UK

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Executive summary.

Clearly stated rights and clearly stated duties are the prerequisite of the relationship between the modern state and its citizens.

The issues of privacy and security are bedevilled by a lack of clarity and huge confusion arising from incoherent and badly drafted legislation covering 14 or more Parliamentary Acts. A statement of basic principles on privacy and security is required.

Basic principles of privacy and security.

A right, such as the right to privacy, is inherent. It is not conferred by the state.

It follows that the duty of the democratic state is to defend and protect the rights of its citizens, not to dilute them.

Enhanced and clearly stated rights are the bedrock of an effective collective defence of the realm in the information age. Any idea of trading off rights for collective security, save in the emergency of war, is a delusion. Diluting rights inverts the relationship between the duty of the state and the rights of its citizens.

Recognising the limitations of state power in the information age,* and knowing that the flow of duty is from the state to the citizen and not the other way round, especially when it comes to the protection of citizens and their rights, is the first step towards a meaningful defence of the country and its citizens by the state in the computer age. We pay the state our taxes to defend us, not to create legislation and bureaucracies that fail in this function.

*See comments of Robert Gates, former US Secretary of Defence, quoted in 'Veil' by Robert Woodward. Simon & Schuster. New York 1987. Page 103

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

The balance between personal privacy and collective security; ISC point 6,a)

1.0 Privacy in the UK

1.1 Privacy is not defined in the statute book. The nearest thing to a definition of privacy is incorporated into Article 8 of the Human Rights Act (1998). Part 1 states that:

Everyone has the right to respect for his private and family life, his home and his correspondence.

This limited principle is diluted to meaninglessness, however, by part 2, which states:

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.

In practice, virtually any activity that a citizen might undertake in an ordinary day is made subject to potential state intrusion on a basis so undefined as to be arbitrary. This makes an ass of the law and implies contemptuous cynicism on the part of the drafting authority. This part of the act, rightly, causes public unease. It is not the 'right' to privacy that the act mandates, merely 'respect' for the right to privacy. It is not stipulated who should pay that respect.

1.3 In the absence of a meaningful definition in the statute book, something along the following lines is needed

Proposed change to the Human Rights Act, Section 8.

Section 1. Delete all and insert 'Every citizen has a right to privacy in their dwellings, in their private lives, in their family lives and in their communications'

Section 2. Delete all and insert 'The state has a duty to ensure that this right is upheld and to make laws that do so. This includes a duty to make such laws as shall ensure the proper functioning of civil order and criminal law and that such laws do not conflict with the basic right to privacy.

(In a recent Computer Weekly survey those most directly affected by the issues, the IT community, had 60% of respondents admit not knowing enough about the issue and 44% stating that privacy and security laws confuse them).

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

The balance between personal privacy and collective security; ISC . 6,a)

2.1 Secrecy in the UK; the Official Secrets Act.

Secrecy in the UK is endemic, pervasive and hugely corrupting, as is any good principle taken too far. Secrecy is the UK is tarnished by its use in recent times to protect officials (The Birmingham 6.75 year seal on documents) to hide possibly criminal acts (Hillsborough) and is now about to face its greatest challenge (See next section, case study) Secrecy in the UK originates historically with the concept of the Crown as the State and the state as an organisation that takes precedence over citizens and their rights. The state, and no person in our country more strongly emphasis this than Her Majesty the Queen, is there to serve the people. Not the other way around.

The Official Secrets Act 1989 moves away from the historical presumption of state precedence up to a point. It is right, and no citizen would object, to Government having a defined and clear capacity to keep certain matters confidential, especially in relation to foreign affairs and defence.

Rather than recommend detailed changes to the Act, it would be better to consider the way the act has failed the UK public in relation to the case study which follows. And to draw up a new act which originates with the principle that the state is there to serve the people and in that service has a need for some secrecy.

The principle of legislative clarity, of having laws that can be understood by a citizen of average education, and of freedom from excessive and confusing legal semantics in statutes, are recommended.

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

3.0 The balance between personal privacy and collective security; ISC . 6,a) The cost and consequences of getting it wrong. A brief case study.

The easiest way to demonstrate what can go wrong, legally, financially, politically and diplomatically when the balance between privacy and security is wrongly struck, when privacy is not respected, and when a state acquires powers that violate basic legal rights, is via a case study of where this has happened.

3. 1 Beginning in 2006 the government of the United States, using a piece of American legislation called the Foreign Intelligence Surveillance Act (FISA 1978), placed orders on a number of American corporations, forcing them to disclose to the National Security Agency, an alien foreign intelligence agency in relation to UK citizens, all their customer data from abroad including but not limited to meta data. This was possible because the FIS Act created secret courts. This enabled the corporations to claim that they were collecting and handing over the data on the basis of 'court orders'. And that they were 'obeying the law'. (See Microsoft letter Appendix)

3.2 The corporations were offered indemnity by the US Government for any consequential financial loss they might suffer. This indemnity may yet cost the US administration vast sums. There are 1.4 billion users of Microsoft Windows. If each user sued for £1,000 and succeeded the final cost would be £1.4 trillion. And for the FISA corporations what is left of their good names and businesses.

3.3 The FIS Act purports to give the US the legal right or power to spy on and in other countries. However, in fact and in law it confers no such powers outside the United States. The assumption that the act could have legal application outside the continental United States and its territories is legally wrong. Surveillance actions taken in almost any other country in the world*, on the basis of FISA, are criminally illegal, and in those countries with treason statutes for spying, carry the death penalty.

3.4 The development of the FISA activity by the NSA via the secret courts has led to the elimination of the entire concept of privacy for the customers of the FISA Corporations abroad. Everything the Corporations could glean about their customers was ordered to be delivered to the NSA, irrespective of any privacy or related laws in the customer's own countries. In the UK this included three principle Acts each of which was violated by the US Corporations who had FISA court orders imposed on them. These are the Human Rights Act (1998) Section 8, the Official Secrets Act Section 1 and the Data Protection Act. (See opinion of Geoffrey Robertson QC, appendix)

3.5 Under the PRISM programme and related programmes authorised by the FIS Act in the USA, but criminally illegal in the UK, all the data of all UK citizens connected to or using the web via the US corporations named in the PRISM programmes, was collected.

Case study/contd

The US Government claim that this is in pursuit of terrorism suspects means that all UK citizens connected to the web are being routinely treated as terrorist suspects by the US. 99.99% of UK citizens have nothing to do with terrorists or terrorism. This raises in the starkest form possible, the question of what all this data is being used for by the NSA ?

3.6 When it discovered the extent to which US high technology companies were able to access the data of the citizens of other states, the US using data collected via PRISM then started to **profile** everyone in those states using data from systems provided by the corporations to their customers. The word profile is the key. The actions of the NSA had almost nothing to do with any legal or legitimate search for terrorists. The NSA was seeking, and has already profiled as many individuals communities and institutions as it could in the UK and elsewhere.

3.7 The ultimate purpose of PRISM and related programme is to enable the US to find ways to influence the profiled individuals, communities and entities, and ultimately to exercise hidden influence and a degree of control over them. While the profiling programme was general across all countries in which the FISA Corporations operated, it had specific targets within the UK. By accessing content and cross referring searches, people who are critical of US policies including MP's, Peers, journalists and academics, are identified. Universities a key target. With the ability to connect individuals with their opinions, private and public, and then to connect them with their search patterns on the web, potentially manipulable profiles are created.

3.8 In a recent extension of the programme, some or all of the UK citizens' financial and tax records have become available to the programme through UK Government departments signing up for cloud databases that are subject to FISA orders. Using the FISA-governed search engines and the cookies created by customers using them, all visits to illicit or embarrassing material is logged. This has given the US the means to use the oldest tool of power, blackmail, on an unprecedented scale mainly against its allies, including the UK.

3.9. **The Official Secrets Act.** This act purports to protect government data, and material deemed secret by HMG. The FISA ordered data gathering failed to make any distinction between data merely protected by the Data Protection Act, the HRA and other acts, and data protected by the OSA. As far as can be ascertained all data accessible to the FISA corporations was transferred back to the NSA, including data allegedly protected by an agreement between the NSA and GCHQ, an agreement that GCHQ had no legal authority to make, without legislative changes.*

3.10 This is what one country has done, having given itself the power, illegally deployed in the UK, to collect all data, almost all entirely 'innocent' data, all of it private, and most of it protected by law.

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Conclusion of the case study. Observation

I think it unlikely that the citizens of the UK want the UK government to have these powers. Further, the intelligence agencies that seek to protect us do not need all this data. The best defence against intrusion and threats against the people of the United Kingdom, is an educated and alert United Kingdom population. Criminalizing the public and diluting their rights is not the way to achieve this.

4. The impact of technology

4.1 The committee asks what difference does technology make to basic legal rights ie privacy and personal data. My answer is; none. I will offer an analogy. It was commonplace in the 19th and early 20th century to have groceries delivered into domestic kitchens. That informal permission did not grant the grocer the right to take things from the household to which he or she delivered goods. Similarly, we do not grant our electricity, gas or water suppliers the right to steal or remove things from our homes, because we are connected to those utilities, even when they come to make repairs. A grant of access is not a grant of the right to thieve. Data is defined as a 'good' in modern law. Stealing data is the same as stealing personal items, such as a watch or wallet.

4.2 Currently if the police want to enter a home, examine a computer, or intercept the mail they get a warrant issued by a magistrate. The obtaining of a warrant is recognition that citizens have basic rights to security, privacy and the sanctity of their homes and communications. These rights have existed in English common law since 1215 and before and are, however badly, reflected in the defective Human Rights Act.

4.3 The presumption of innocence before the law is and must remain absolute. The granting of the right to collect general data violates this principle as well as the others. It presumes the whole population guilty. Technological capacity does not erode basic civil or constitutional rights. Arguments that it does are wholly specious.

5.0. The Data Protection Act

This is a perfect example of a total statutory wreck, one that merely adds to the sum of public cynicism about law and government.

5.1 The Act is over 212 sections long, (74 pages plus further schedules) yet it confers no easy or clear right on a data subject (citizen) to pursue breaches of the principle by him or herself, at reasonable cost, in a county court.

5.2 The Agent of the Act, the Information Commissioner, who in theory represents the individual and is there to enforce the Act, cannot do so. The Information Commissioner has proved helpless and powerless in the face of the actions of the FISA Corporations in the UK. His duties, as actually defined in the act, prevent him from doing anything effective. The position is a bureaucratic nonsense, the logical consequence of a totally confused statute.

5.3 Every potential right a citizen has to proper possession of his or her own data is neutralised and made ineffective by what constitutes a 'walk away with all UK data, including government data, get out of jail card'.

According to the Information Commissioners Office, the following exemptions to any protection offered by the DPA (The Information Commissioner commenting on the Schedule 7 exemptions) "Personal data is exempt from the non-disclosure provisions if you are required to disclose it:

- by or under any UK enactment;
- by any rule of common law; or
- **by an order of a court or tribunal in any jurisdiction.**

In these circumstances, the legal obligation overrides any objection the individuals may have."

The FISA corporations are offered the perfect loophole in the last item. It is a common demonstration of how bureaucracy can destroy basic citizen rights using a badly written statute.

5.4 Legislative proposal regarding amendment of the Data Protection Act.

The Act should be rewritten. Data should be defined in terms of owner's rights, deriving directly from a suitably amended Article 8 rights. Remove the Information Commissioner and appoint in the Act an authority that investigates, enforces and penalises breaches of the Act. Close all loopholes, and provide a procedure that is accessible and affordable by ordinary citizens in the County Court.

6.0 Metadata v content

The committee has raised an issue distinguishing 'facts about a call' and the 'content of the call '. The content of a call is a private communication, and should be covered by the amended Human Rights Act and Data Protection Act. The making of a call, e-mail or any other communication is a private act and should never confer a right on anyone to collect data on calls made and, more importantly, web searches, without the consent of the owner, or unless with a warrant on the basis of reasonable suspicion. Where cookies are used for illegal purposes, namely for the purpose of being passed to a foreign intelligence service, any foreign intelligence service, this should be made a specific criminal offence.

6.1. China and Russia long ago protected their own populations from US intrusion , because they understood what the US was doing. The basic devices used are the firewalls so frequently complained of by the Western media, who never bothered to investigate what the US itself was doing.Both countries have extensive supercomputer facilities and staff to match. But one party and totalitarian states have almost certainly used the same profiling techniques the US uses, against their own populations. Such is the nature of totalitarianism.

Sources

The information above, about what the US was doing with the data, was widely known, if in an unfocused way, in the supercomputer fraternity, of which I am a member*. It was talked about informally at the annual International Supercomputer Conferences, which I have attended regularly for the past 20 years. It is also easily discernable to a professional systems analyst in the PRISM memos themselves, published by the Guardian on the 6th, 7th and 8th June 2013. That is where the issue came into focus.

I do have personal sources, of course. But they have merely confirmed what is visible in the Snowden evidence, especially that relating to PRISM.

Ends

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Appendix A

Expansion of Kevin Cahill's expertise in intelligence related supercomputing fields.

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Appendix A

Personal locus for addressing the committee, expanded.

I am a former army infantry officer. I did the Sandhurst 'long' 2 year course, Intake 35 Sept 1963 to July 1965. I served in Aden, Bahrain and finally in Northern Ireland. I have direct, personal experience of terrorism. I remain an active member of the Sandhurst Trust. After I left the Army in 1968 I joined the computer industry and became a systems analyst. That professional skill is crucial to the way I approach the issues raised by the committee; systems analysis is the key professional skill employed in all modern intelligence analysis. In 1979 I became the international and financial editor of Computer Weekly, a computer trade magazine with a weekly printed circulation of 100,000. This gave me unique access to the world of international computing and its two greatest engineers; Dr Gene Amdahl FBCS and Dr Seymour Cray FBCS.

I became a professional friend of Dr Amdahl, and thanks to him, became a non technical expert on supercomputers, their design and software, but mainly their application. On the I8th April 2012 I sponsored Europe's most eminent supercomputer expert the late Professor Dr Hans Meuer, Chair of the annual International Supercomputer Conference, at a lecture in Committee Room G of the House of Lords*. I subsequently authored the Computer Weekly guide to supercomputing (2012) attached *. Supercomputers underpin all modern intelligence work.

Between 1984 and 1988 I was the Rt. Hon Lord Ashdown's part time researcher in the House of Commons. Lord Ashdown is a former Royal Marine officer, and a former M16 station chief (See his autobiography) He asked me to join him following a story I wrote about violations of UK sovereignty by the computer company IBM acting on behalf of the US Government .* Ultimately I wrote a book about the illegalities called Trade Wars. There are copies in the House of Commons library. There were about 2,700 press cuttings about the issue and two TV documentaries. 'Technology Wars' C4 Despatches and 'Uncle Sam's Law'. Thames TV Eye.

Trade Wars is an account of the legal and administrative issues involved in day to day sovereignty in the United Kingdom. As such it addresses the issues implicit in the issues the committee raises about individual and collective security. It also addresses a related issue of huge public concern; this is the role of our most important strategic political and military ally, the United States, in the role of intelligence surveillance, especially inside the United Kingdom.

The book 'Who Owns the World' required that I read the constitutions of 197 countries; about 98% of the world's countries. The book dealt with basic structures of law and rights in all those places as well as land. It has given me a planetary perspective on the world, its peoples and their rights.

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Appendix B

Invitation by Professor the Lord Laird of Artigarvan to (the late) Professor Dr Hans Meuer to lecture in Committee Room G of the House of Lords on 18 April 2012 to lecture on the topic of

Supercomputers - Prestige Objects or Crucial Tools in Science and Industry

From Professor the Lord Laird of Artigarvan FRSA, FCIPR

7th April 2012

It gives me great pleasure to invite you to

The Second Lorraine King Memorial Lecture

Sponsored by Kevin Cahill FRSA, FRGS, FBCS.CITP, FRHistS

in

Committee Room G of the House of Lords on 18th April 2012 at 1900

Given by

Professor Dr. Hans Werner Meuer

University of Mannheim and Chair of the International Supercomputer Conference 2012

On the topic of

"Supercomputers –Prestige Objects or Crucial Tools in Science and Industry "

Supercomputers are strategic devices that are having a huge impact on many areas of modern life, including advanced science, weather forecasting, manufacturing productivity, cancer research and computing itself . The United Kingdom is well represented as a user in this field as the attached table shows, but more could be done. For example, only France in Europe has a serial manufacturer of Supercomputers. This is an issue that Professor Meuer will address in his talk.

In Japan the Riken K computer is more than three and a half times faster and more powerful than any other computer on earth. It has been built at the Riken institute with the specific task of helping Japan to deal with a series of issues common to many countries, including aging population, medicine, weather and catastrophic incident forecasting. We in Europe can learn a great deal from the way the K machine has been augmented on site by so many other activities relating to science and technology.

Professor Meuer runs one of the largest annual Supercomputer conferences in the world and is credited with keeping the spirit of Supercomputing alive and thriving in Europe. In the discussion that will follow Professor Meuer's talk I would like to address both the issue of a UK Supercomputer Conference to complement his gathering in Germany and a Specialist Supercomputing Group at the British Computer Society.

Attendance..

The talk will take place in Committee Room G of the House of Lords. Entry is by numbered invitation only. Your invitation should be presented to the Security staff at Black Rod's Garden Entrance, at the western end of the Palace of Westminster. The nearest tube is Westminster and there is an NCP car park nearby. Allow a little time to pass through security. Please bring some form of photo identification with you. The talk starts with a short reception at 1900, and will conclude at 2100. Dress is normal business dress. (No map is attached apologies) If you wish to appoint a substitute attendee, please advise me by e mail.

ros@globalnet.co.uk

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Appendix C

Computer Weekly supercomputer survey for 2012 by Kevin Cahill

This was survey of supercomputers in all 27 countries in which they had been installed up to 2012, together with details of applications, comparative distributions and power rating table for the top 10. The UK does not appear amongst the top 10, has no native manufacturer of supercomputers and buys most of its machines together with the conditions evidenced in the IBM letter in the history section of these appendices.

A Computer Weekly guide to supercomputers

At the forefront of technological advancements, supercomputing and its far reaching potential is hindered only by the shortcomings of the humans employed to utilise it, writes Kevin Cahill

The supercomputer sector is the fastest growing niche in the technology world, with annualised installation growth of over 10% to date.

The overall supercomputer market in 2012 was worth $25.6bn, 22% up on the previous year. Annual growth to 2015 is forecast at 7% per annum, according to figures from the High Performance Computing (HPC) Advisory Council.

The average cost of an installed machine is between $10m and $20m, but for some of the bigger sites it is upwards of $100m, and can exceed $200m.

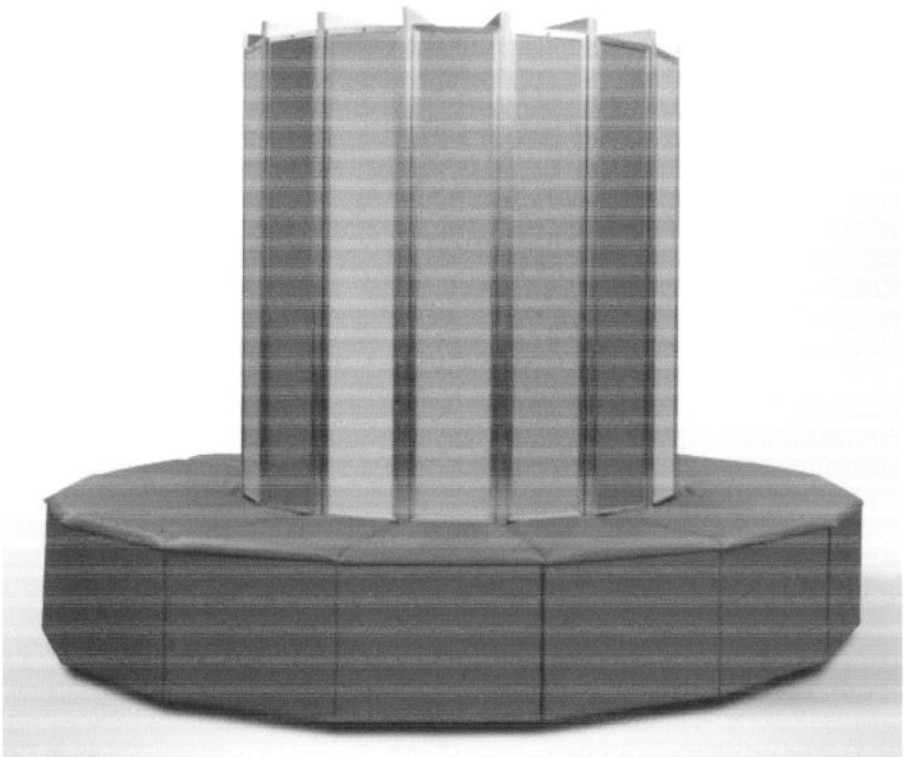
By definition a supercomputer is the largest, most powerful (fastest) computer available at any given moment in time. In practice supercomputers are scientific and numerical processors, rather than data processing machines.

They are built on a different basis to data processing machines, and are many times faster. The power of a supercomputer is measured several ways, but flops (floating-point operations per second), is the current measure.

The Top 500 rankings of the most powerful computers are based on a commonly accepted test, called a Linpack. This measures the speed at which a machine executes a dense system of linear equations. The run rate is commonly reported in flops. The current top machines are in the teraflop zone, at 10 to the power of 12 flops. The big race is to get to an exaflop machine (10 to the power of 18) by 2018.

Three design teams, in the US, Japan and China, are attempting to win the race. The breakthrough machine will be called the exaflop machine, a device that can do tens of trillions

The US Cray 1 supercomputer



About the author

Kevin Cahill *FBCS, CITP (FRSA, FRGS, FRHistS)* is a professional Fellow of the British Computer Society, a former confidante of Dr Gene Amdahl and former finance, later international editor, of Computer Weekly. Subsequently he was deputy editor and supercomputer correspondent at Computer News.

He was later deputy editor of the Sunday Times Rich List and has recently written cover stories for the New Statesman on land ownership on which he is the world authority through his book 'Who Owns the World'.

Kevin Cahill is a special advisor in the House of Lords and a Fellow of the Royal Society for the Arts, a Fellow of the Royal Geographical Society and a Fellow of the Royal Historical Society. He lives in Devon.

A supercomputer is the largest, most powerful computer available at any given moment in time

of calculations per second and which will close down a small city, when it is switched on (20 MW of power needed. It will run at a rate of 10 to the 18 flops.) It will be the largest, most complex device ever constructed by mankind.

The supercomputer community

There are approximately 500,000 people working within the supercomputer sector. The majority work with installed machines, applying them to specific, real world problems. But there is a significant group working in the construction of the machines, and on research and development associated with them.

There is a vast skills shortage in the sector. It is at its most acute in the area known as operating systems. This is the software that controls the machine and connects it to the application software that actually does real world work, such as modelling the planetary weather system.

The electronics have moved so far ahead of the software that the situation has been likened to having a Ferrari engine with a model T Ford three speed manual gearbox to get the power to the wheels, which have yet to move on from the equivalent of solid rubber to pneumatic tyres.

The rule of thumb that applied to all earlier computers, that what you get out is only as good as what you put in, applies in spades to supercomputers. If you use bad data you get bad data back, only faster and worse.

There is a further issue, not much discussed in the industry. Supercomputers are not data processing machines and use models, mathematical formula and other intellectual creations to work on problems. Those programmes are equally subject to the earlier observation. Bad programmes deliver bad results, only much faster. The machines expose flaws in human thinking, and do so at great speed. The internal ethos in the industry is a unique blend of pure science, and applied engineering.

User skill shortage famously resulted in the failure of the Japanese Earth Simulator supercomputer to forecast or predict the 2011 Tsunami. And the failure of the many machines in the banking structure to forecast the sub prime crash. Rather, banking staffs appear to have used their supercomputing power to accelerate the pace of the crisis and make it worse.

The strategic importance of supercomputers

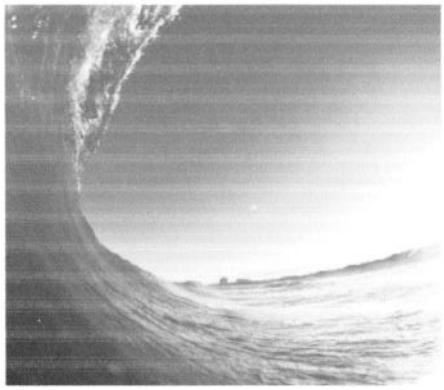
After nuclear weapons the most important strategic devices on planet earth are supercomputers. They will determine the success or failure of countries, continents even, for the whole of the future. Without them, mankind itself may not be able to survive.

The competition for pole position; possession of the largest, fastest and most powerful supercomputer, lies between just three countries; Japan, China and the US, and the competition is intense. Japan currently holds the lead, China is second and the US third.

Unusually, the key teams are accessible, at least to conference visitors. Members of all three teams attended the International Supercomputer Conference (ISC 2011) in Hamburg and there were open sessions with the designers, very akin to academic conferences.

The level of secrecy that might have been expected did not occur. This is partly explained by the fact that the kinds of problems that these three teams are trying to solve, in creating the ultimate machine, are beyond either individuals or countries to resolve.

Note the power gap between 1 and 2 in Table 1 below showing the top 10 machines globally.



The Japanese Earth Simulator only failed to predict the 2011 tsunami due to user skill shortage

Table 1: Top 10 of the Top 500 machines by power and by country

No.	Country	Machine	Power RMax (measure of speed)
1	Japan	Riken K	11,280
2	China	NUDT	4,701
3	USA	Cray (XT5)	2,331
4	China	Dawning	2,984
5	Japan	NEC/HP	2,287
6	USA	Cray (XE6 custom)	1,365
7	USA	SGI	1,315
8	USA	Cray (XE6 custom)	1,288
9	France	Bull	1,254
10	USA	IBM	(1,200)

Source: Top 500 List, Nov 2011

"Supercomputers will determine the success or failure of countries, continents even, for the whole of the future. Without them, mankind itself may not be able to survive"

Top supercomputer sites

Four key individuals within the industry, Hans Meuer, Jack Dongerra, and two others, have produced a twice yearly listing of the 500 largest supercomputers worldwide.

There are probably between 1,000 and 2,000 operational supercomputer sites worldwide, outside the top 500 sites. The largest supercomputer community is in the US, where more than 50% of all supercomputer sites are based.

There is no accurate figure for the staffing of supercomputer sites, but 150 to 200 staff per site is a reasonable estimate from the known data. The total potential supercomputer community worldwide is between 375,000 and 500,000 people. Almost all supercomputer staff are graduates, mostly science, and it's fair to assume that the majority hold PhD's.

Growth in employment at R&D and manufacturing end of industry

Increase in overall employment is forecast at 35,000pa or 175,000 over five years to 2015.

However, the shortage of technical staff at manufacturing and research sites may be as high as 50% and is probably higher in operating system level software development. There is an even more severe shortage of staff at the user end, especially of qualified staff to apply the machines. This is estimated to be somewhere between 25% and 50%.

These two estimates suggest that actual growth needs to be close to 10-12% to fill existing gaps and to improve the level of application success and productivity. This would result in a growth of employment in the sector by 250,000 to 2015. There are no estimates for the associated growth in jobs and ancillary employment as supercomputer sites generate new products and new applications.

Published May 2011, the above figures are derived from the HPC Advisory Council estimates.

Table 2: Country distribution of the Top 500.

Rank	Country	Number of Top 500 Supercomputers	% of installed base	Per million head of population
1	United States	263	52.6	1.1
2	China	74	14.8	17.5
3	Japan	30	6	4.2
4	United Kingdom	27	5.4	2.2
5	France	23	4.6	2.8
6	Germany	20	4	4.0
7	Canada	9	1.8	3.6
8	Poland	6	1.2	6.3
9	Russia	5	1	28.6
10	Australia	4	0.8	5.5
11	Italy	4	0.8	15.0
12	South Korea	3	0.6	16
13	Israel	3	0.6	2.6
14	Ireland	3	0.6	1.5
15	Switzerland	3	0.6	2.6
16	Sweden	3	0.6	3.1
17	Saudi Arabia	3	0.6	9
18	Spain	3	0.6	15.3
19	Brazil	2	0.4	96
20	Taiwan	2	0.4	11.5
21	Austria	2	0.4	4.2
22	India	2	0.4	600
23	Denmark	2	0.4	2.75
24	South Africa	1	0.2	50
25	Finland	1	0.2	5
26	Belgium	1	0.2	10
27	Singapore	1	0.2	5

Source: Top 500 list

Supercomputing skills shortages

There is a vast skills shortage in the sector. It is at its most acute in the area known as operating systems. This is the software that controls the machine and connects it to the application software that actually does real world work, such as modelling the planetary weather system.

The electronics have moved so far ahead of the software that the situation has been likened to having a Ferrari engine with a model T Ford three-speed manual gearbox, to get the power to the wheels, which have yet to move on from the equivalent of solid rubber to pneumatic tyres.

The rule of thumb that applied to all earlier computers, that what you get out is only as good as what you put in, applies in spades to supercomputers. If you use bad data you get bad data back, only faster and worse.

Table 3: Top 500 supercomputers ranked per million of the population				
Rank	Country	Number of Top 500 Supercomputers	% of installed base	Per million head of population
1	United States	263	52.6	1.1
2	Ireland	3	0.6	1.5
3	United Kingdom	27	5.4	2.2
4	Israel	3	0.6	2.6
5	Switzerland	3	0.6	2.6
6	Denmark	2	0.4	2.75
7	France	23	4.6	2.8
8	Sweden	3	0.6	3.1
9	Canada	9	1.8	3.6
10	Germany	20	4	4.0
11	Japan	30	6	4.2
12	Austria	2	0.4	4.2
13	Finland	1	0.2	5
14	Singapore	1	0.2	5
15	Australia	4	0.8	5.5
16	Poland	6	1.2	6.3
17	Saudi Arabia	3	0.6	9
18	Belgium	1	0.2	10
19	Taiwan	2	0.4	11.5
20	Italy	4	0.8	15.0
21	Spain	3	0.6	15.3
22	South Korea	3	0.6	16
23	China	74	14.8	17.5
24	Russia	5	1	28.6
25	South Africa	1	0.2	50
26	Brazil	2	0.4	96
27	India	2	0.4	600
Source: Top 500 list				

At upwards of $10m to $20m per machine, and ignoring the colossal cost of running a site, all decisions about purchase or commission are made at board or government cabinet level

Vendors and manufacturers

There are only 11 companies that can be said to be serious producers of installable supercomputers; IBM, Hewlett-Packard, Cray, SGI, Bull, Appro, Dell, Hitachi, NEC, Fujitsu and Dawning, out of a world total of 37 producers. These companies are concentrated in the US, Japan and China.

Table 4 shows how well the national super computer strategies are working out. It shows how dominant one American company, IBM is, and how poorly the Chinese serial producer, Dawning, is doing. Likewise it shows how poorly the Japanese are doing.

Market for applications and peripherals

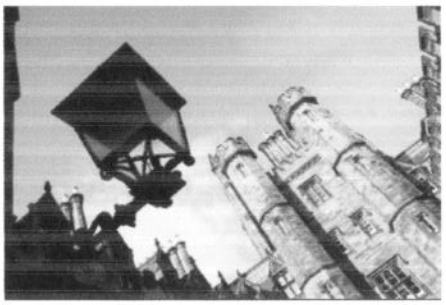
The sector remains under marketed, because despite IBM's best efforts, it is not a mass market. At upwards of $10m to $20m per machine, and ignoring the colossal cost of running a site, all decisions about purchase or commission are made at board or government cabinet level.

Based on revenue breakdown estimates to 2015 produced by the High Performance Computing (HPC) Advisory Council and out of a total estimate of revenues for the industry of $35.5bn that year, the following peripherals and support technologies are forecast to achieve the revenues, and staffing uplifts as detailed in Table 5.

The application sectors, as outlined in Table 6, are mainly selling sub capital additions to machines. Marketing expenditure and activity is likely to increase significantly here.

Universities. Key focus for expansion

Looking at the top site in the UK, that at Edinburgh University, we can see this as an indicator of where governments on the one hand, and vendors on the other, will focus their attempts to expand the market. Governments will be looking to improve job opportunities for their graduate populations and get greater efficiencies in their economies. Vendors will be looking to install a mid-range machine in 10% of the world's approximate 8,000 universities.



Edinburgh University is the top supercomputer site in the UK

Key decision makers

In this sector the number of key decision makers is very small. The boards of the Fortune 500 companies in the US and the boards of the FTSE 100 companies in the UK. In most of the 27 top 500 countries up to half the decisions are made by government. And the vendors will be looking to expand the market by getting machines into more countries.

The impact of supercomputers on (small) economies

It is too early to give definitive figures for the impact of supercomputers on a given country's economy. No attempt has been made to collect or correlate data and so far no economists, apart from Ricardo Hausmann at Harvard, have even begun to see the relationship between future high rate economic growth and the drivers in the knowledge based economy. The emergent key drivers are likely to be supercomputers.

IBM is leading the way with over 50% market share

Table 4: The supercomputer suppliers and the number of machines appearing in the Top 500 list

Rank	Name	Country	Machines in top 500	What you need to know
1	IBM	USA	223	The ultimate competitor with over 50% total market share
2	Hewlett Packard	USA	141	The challenger to the top spot and a serious contender
3	Cray Inc	USA	27	Ambitious start-up fuelled by Pentagon funds; seriously clever machines
4	SGI	USA	17	University focused
5	Bull	France	15	France focused
6	Appro	USA	13	A rising star
7	Dell	USA	11	Ambitious micro dealer
8	Oracle	USA	10	Needs supercomputing power to run its software
9	Hitachi	Japan	5	Part of the Riken/Japan project
10	Fujitsu	Japan	4	Japan's original white hot hope
11	NRCPCET	China	3	China's current market leader
12	NUDT	China	2	The competing Chinese rival to its current market leader
13	Dawning	China	2	China's targeted serial manufacturer
14	Dell/Sun/IBM	USA	2	A research focused rather than commercial offering
15	NEC	Japan	2	Biggish legacy base with SX series machines
16	Atipa	USA	2	Integrator
17	Self made	------	2	----------
18	IPE, NVIDIA, Tyan	China	1	Part of the China plan
19	Clustervision Supermicro	USA	1	Too small to be a contender.
20	Acer Group	Taiwan	1	Keen outsider with government support
21	Supermicro	UK	1	Very small scale
22	Lenovo	China	1	Outsider in China. Big in micros
23	Inspur	China	1	Not widely known, but ambitious
24	Xenon Systems	Australia	1	Ambitious integrator
25	Clustervision/Dell	USA	1	Joint venture
26	Penguin Computing	USA	1	Integrator
27	NEC/HP	Japan	1	Experimental joint venture
28	T. Platforms	Russia	1	May be the Russian domestic hopeful
29	Megware/ASUS	Australia	1	Integrator
30	Raytheon/Aspen	USA	1	Experimental
31	Intel	USA	1	Needs to know how its chips are used
32	RSC SKIF	Russia	1	Russian outsider
33	NSSOL/SGI Japan	Vietnam	1	Interesting peripheral player
34	Asus	Australia	1	Integrator
35	ACTION	Poland	1	Polish hopeful
36	Dell/Oracle	USA	1	Experimental joint venture

Source: Top 500 list, Nov 2011

Ireland ranks 2nd in the world in terms of supercomputer installations per million of the population. Ireland had a trade surplus of €21.3bn in the 1st half of 2011, together with a drop in labour costs of 3.5%. These are the two indicators that should emerge to prominence, if supercomputers are having the predicted effect.

Conferences and websites

There is no industry website or trade magazine as such. The industry gets together at two big conferences; one in Germany (2,600 attendees) and one in the US (3,000 to 6,000 attendees). The extraordinary competition between the US, China and Japan at the top has trickled down to make this one of the most competitive and ego driven industries on earth.

The majority of personnel in the sector are conscious of being at the leading edge of planetary engineering and applied science. The machines they create have made the human genome project feasible, have led to advances in medicine and pharmacy unforeseen even 10 years ago and have only just begun to make an impact that will change everything on planet earth itself. They make the machines that will remake our entire experience of living on planet earth.

Table 5: HPC Advisory Council growth estimates for the sector	Revenue growth	Community size growth
Machines themselves	$12.5bn	na
Storage	$6.5bn	10,000
Services	$5.0bn	20,000
Software	$7.5bn	15,000
Networks	$2.0bn	5,000
Other	$2.9bn	5,000
Source: HPC Advisory Council, May 2011		

Table 6: Supercomputer Applications			
Application area	No. of machines	%	No of personnel
Not specified	238	47.6	47,600
Research (University)	71	14.2	14,200
Finance	24	4.8	4,800
Service	21	4.2	4,200
Logistics	21	4.2	4,200
Defence	16	3.2	3,200
World Wide Weather	15	3	3,000
Geophysics	13	2.6	2,600
Information services	10	2	2,000
Energy	10	2	2,000
Climate research	10	2	2,000
Aerospace	8	1.6	1,600
Benchmarking	7	1.4	1,400
Telecomms	6	1.2	1,200
Internet provider	5	1	1,000
Transportation	5	1	1,000
Info Processing Svc	5	1	1,000
Automotive	2	0.4	400
Medicine	2	0.4	400
Software	2	0.4	400
Weather forecasting	2	0.4	400
Electronics	2	0.4	400
Digital media	1	0.2	200
Life science	1	0.2	200
Environment	1	0.2	200
Semiconductor	1	0.2	200
Biology	1	0.2	200
Source: Top 500 list			

About the HPC Advisory Council

The HPC Advisory Council's mission is to bridge the gap between high-performance computing (HPC) use and its potential, bring the beneficial capabilities of HPC to new users for better research, education, innovation and product manufacturing, bring users the expertise needed to operate HPC systems, provide application designers with the tools needed to enable parallel computing, and to strengthen the qualification and integration of HPC system products.

Source: HPC Advisory Council website

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Appendix D

The legal opinion of Geoffrey Robertson QC in relation to the FISA Corporation illegalities.

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

Appendix D

The following opinion of Geoffrey Robertson QC, of Doughty Street Chambers, appeared in Computer Weekly on the 6th Dec 2013.

He was commenting on the commencement of the first civil cases in UK courts against 3 of the FISA Corporations .

Human rights lawyer Geoffrey Robertson QC said the action could have far-reaching consequences for Microsoft and other service providers, if it succeeds.

"Microsoft allegedly betrayed its customers by providing their personal information, without their consent, to the NSA," said Robertson.

"This would constitute a serious breach of the British Data Protection Act, by an American company putting its allegiance to America above its legal duties to its British customers."

Invasion of privacy

Robertson said breaches of the Data Protection Act should be treated as seriously as the *News of the World*phone hacking case.

"The invasion of privacy, by deliberately declining to obtain a customer's consent before exposing their personal details to another, deserves to be compensated on the same basis as obtaining personal data by hacking mobile telephones," Robertson said.

The Intelligence and Security Committee of Parliament
Privacy and Security Inquiry February 2014.

Evidence of Kevin Cahill.

History of UK trade illegalities in the UK

For many years US corporations have sold computers, especially supercomputers, in the UK with US government conditions attached that have been deemed in breach of UK Sovereignty by a range of UK Government Ministers, including Prime Minister Thatcher.

The Garvey Memorandum April 12 1956. From the book Trade Wars by Kevin Cahill

Tom, later Sir Tom Garvey in this memo relating to high tech trade with the then East Bloc, used a phrase ' forcible federalisation' in relation to the United States. This phrase has not appeared elsewhere and is assumed to refer to a post World War 11 arrangement forced on the Allies and the UK, by the US. No historian has been able to explain what Garvey meant. Perhaps its time we found out ?

The IBM letter of 22 December 1983.

In this letter IBM made clear to its customers that they could not move their advanced computers around the UK without approval of the US Government. This was deemed a violation of UK Sovereignty by the President of the Board of Trade, Norman, now Lord Tebitt, the Attorney General Sir Michael Havers and by the Prime Minister.

The Prime Minister's letter of 11 November 1988 to Paddy Ashdown MP

In this letter, the last in a series of 8 on the topic of the US violation of Sovereignty the Prime Minster makes clear what she can do about the matter. Nothing. Perhaps we should know why ?

SHOTGUN DIPLOMACY

Telegrams Nos. 1534 and 1535 to Washington, of which I attach copies, represent the latest move in the campaign for reducing East-West trade controls. To clinch the argument the President of the Board of Trade reverts to his favourite theme that, if the Americans do not accept our point of view, and that quickly, we shall advertise our disagreement to the other dozen or so members of the Paris Group, and endeavour to unite the Europeans against the United States. I think it is fair to describe this as the "favourite theme" of the President of the Board of Trade, since he has been playing variations upon it ever since March 22 (see this minute to the Prime Minister of that date at Flag A), and he continued to do so throughout the conversations in London with Mr. Stassen and M. Schumann at the beginning of this month.

2. This policy of holding the Americans up to ransom is not, as might be thought, some aberration of the President's, resulting from lack of coordination between the Board of Trade and the Foreign Office. On the contrary, the commercial appetites of the Board of Trade have been harnessed to the Prime Minister's notions about domesticating the Russians by turning the U.S.S.R. into a welfare state, and about the possibility of "friendly infiltration" through trade: with the result that it is now evidently the considered policy of H.M. Government to go after a massive reduction of strategic export controls regardless of the consequences elsewhere.

3. It is not the purpose of this minute to suggest that we should attempt here and now to reverse this state of affairs. The present policy has been opposed by the Foreign Office all along the line, but we have been steadily defeated. We should however not delude ourselves that it is a right policy, and should be on the alert for any turn of events which might enable us to reverse it.

4. The case for not behaving as, under the impulse of the President and the Prime Minister, we have recently been behaving, is this. Britain claims, in her dealings with the United States, what we have frequently called a "special relationship". This is, in a small measure, a matter of sentiment (common ancestry, common law, etc.,), but rests mainly with a certain amount of justification, to be America's only reliable ally, the only one that will fight, the only one that really tightens its belt and so on. The Americans also rely on us quite a bit, though they do not admit it, for political know-how and common sense. It is on the basis of our "special relationship" founded upon these real, or supposed, qualities that we have had the Loan, the lion's share of Marshall Aid, comparative immunity from forcible federalisation, and so on.

5. Few things could be more destructive of the "special relationship" than a demonstration, on a matter of real importance to the United States Government, that Britain is not merely in herself no better than the squalling and selfish Europeans, who are continually trying to blackmail and brow-beat the United States into doing things for them, but is also prepared to desert the side of the United States, and rouse the Europeans to revolt against her.

6. It has always been the custom for the business of the Paris Group to be pre-digested at an Anglo-American meeting a few days in advance. Thereafter, the two of us have squared the French (who hold the Chair in the Group), and thereafter i has generally not been too difficult to get the right decision from the plenary. It is against this background of especially close Anglo-American consultation that Mr. Thorneycroft's tactic of threatening to raise the crew to mutiny must be judged. Nor indeed is this matter one on which the United States Government have much latitude. Mr. Stassen has by a skilful publicity campaign improved the atmosphere very markedly in the last twelve months. But American opinion is simply not ready for a de-control of East-West trade on the lines which commend themselves to Ministers here, and pressure on the Administration, while undermining our relationship and weakening our general bargaining position, is unlikely even so to achieve its objective.

T.W. Garvey
April 12, 1954

Mr Garvey is quite right to draw attention to this danger. It has not arisen yet. But it may, if the President of the Board of Trade does not consider that Mr. Stassen's reply is satisfactory.

In that case I take it that there can be no question of our tabling our short list on machine tools and rolling mill items without the question being considered by Ministers. In a previous minute you agreed that such proposed action should go to the Secretary of State personally before it was taken. On that occasion it related to the whole list. But in my own view it should equally apply to the present list of machine tools and rolling mill items, which is a very important section of the whole.

Lord Reading
March 14, 1953.

policy?

IBM United Kingdom Limited

IBM South Bank
76 Upper Ground
London SE1 9PZ
Telephone: London (01) 928 1777
Telex: 919039 (IBMSBK G)

IBM & Esprit.

22 December 1983

US EXPORT REGULATIONS - "ADVANCED SYSTEMS"

Some recent Press reports about the effect of US Export Regulations on computer equipment have tended to be concerned with exports from the United Kingdom.

As you are aware, transactions within the United Kingdom involving "Advanced Systems" are also subject to the obtaining of US export licence approval. Such transactions include not only the initial installation of a new machine with a user, but also any subsequent dealings or transfers in such machines (at least while they remain an "Advanced System").

The following is a list of the IBM machines for which individual licences are currently necessary, in the case of UK installations:-

3033, 3033N, 3033S
3042 (Attached Processor for 3033, 3033N and 3033S)
3062 (Attached Processor for 3168)
3081
3083
3168
3195
3838
3084 (including 3081K to 3084 upgrade)
4381 model Group 2

Accordingly, I would like through this letter to remind you in particular that transfers between users of any machines listed above at present require US export licence approval before installation at the new user's site. You should allow sufficient time (in some cases up to

three months) for applications to be processed. The appropriate licences can be obtained from the US Department of Commerce, either directly in Washington DC, USA, or via the US Embassy in London. The address in Washington is:-

Director, Office of Export Administration,
US Department of Commerce
International Trade Administration
Office of Export Administration
PO Box 273
Washington, DC 20044
USA
Telex No: 892536 (USA)
Telephone: (202) - 377 - 4811

US export licence approval will of course also be required in the case of any transfers of such machines from the UK to users in countries other than the US or Canada. Further, all such exports are also licensable by the Department of Trade.

Please let me know if I can clarify these requirements further.

Yours sincerely

M CARTER
Branch Manager
Computer Related Industries Branch
dch08aa

10 DOWNING STREET
LONDON SW1A 2AA

THE PRIME MINISTER

11 November 1988

Dear Mr. Ashdown,

Thank you for your letter of 17 October which responded to my letter to you of 11 August.

I can assure you that the Government's policy on extravagant US claims to extraterritorial jurisdiction has not changed. You will no doubt recall that, in his letter to you of 3 July 1985, Michael Havers warned that, although US claims to extraterritorial jurisdiction are offensive, it is only realistic to recognise that we cannot in practice compel the US to stop making such claims and seeking to enforce them. Michael further explained that it is necessary to consider whether use of the Protection of Trading Interests Act in a particular case would be likely, on balance, to benefit UK trading and commercial interests, and that the Government's judgment has been that, in these difficult circumstances, UK firms and individuals should generally be allowed to make a commercial judgment about whether to comply with US licensing requirements and any subsequent enforcement action. My letter of 11 August did not imply that there has been any change in this policy; nor has there been.

I do not accept that my letter gives rise to the two questions you have raised. On contracts, the Government's position remains as in the Diplomatic Note of 18 October 1982; on Distribution Licences, our position remains as

stated in the answers given by Paul Channon on 19 February 1987 (Official Report, Column 751) and Alan Clark on 24 February 1987 (Official Report, Column 206).

The Government are aware of problems regarding the supply of software to academic institutions. The Departments of Trade and Industry and Education have been having discussions with the US Department of Commerce for some time in an attempt to ease this situation. In particular, the Government has contributed representations to a US review of that part of the Export Administration Regulations which concerns export controls on technical data and software, repeating our objections to the extraterritorial imposition of re-export controls and advising the US of limitations which such controls might impose on the sale of US products to the UK. I also understand that, in response to US controls on software, universities in this country are considering funding development of programmes comparable to those supplied by US software distributors. This is not an immediate solution, but it should benefit the UK in the longer term, while any loss of business by US suppliers should also increase the pressure for change to US Export Regulations.

Yours sincerely

Margaret Thatcher

Paddy Ashdown, Esq., M.P.