[Brian E. Carpenter]Brian E. Carpenter: Internet

Dr. Brian E. Carpenter, http://www.cs.auckland.ac.nz/~brian, *is a distinguished computer scientist and engineer working on Internet standards and technology. The University of Auckland was privileged to attract Brian in 2007, and he was appointed Professor in 2009. Before coming to Auckland, he led the networking group at CERN, the European Laboratory for Particle Physics, and worked for IBM as a Distinguished Engineer. During his career he has published in various areas: automatic speech recognition, control software, programming languages, networking and the history of computing. Brian chaired the Internet Architecture Board, the Internet Engineering Task Force, and served as a trustee of the Internet Society. Brian was heavily involved in the design and deployment of IPv6. He is also interested in Internet quality of service, management and measurement issues. Brian was a member of the IBM Academy of Technology (membership lapses when one leaves IBM).*

This interview was originally conducted in 2008, and has been resumed in 2014. Some additional answers, and some new questions, have been added with the benefit of hindsight.

CC:: Can you please succinctly describe the history of the Internet?

BC:: That's a tall order, but here goes. Packet switching was invented in the 1960's, by Paul Baran in the US and independently by Donald Davies in the UK. Various packet switching networks were prototyped, most famously the ARPANET starting in 1969. In the early 1970's, the idea of interconnecting networks (hence *inter-net*) using a single logical addressing scheme and a common packet format was raised by Louis Pouzin in France, and rapidly adopted by the ARPANET community. This led to the pioneering design of TCP/IP by Vint Cerf and Bob Kahn, which was also the first clear example of a layered protocol stack. TCP/IP was deployed on the ARPANET on January 1st, 1983 and one can say that the Internet has existed since that day.

A key event was the availability of free TCP/IP software in the Berkeley Unix distribution 4.2BSD, also in 1983, which led to its rapid spread throughout the academic community and the emerging personal workstation market. As the 1980's progressed, there was an era of protocol wars, in which TCP/IP fought against proprietary protocols and against the "official" standards emerging from the ITU and ISO. TCP/IP won for a variety of pragmatic reasons. At the same time, international connectivity appeared, spurred on by the continued progress of Unix in the academic world, and the appetite for collaboration. For example, the first "high-speed" transatlantic link, at 1.5 Mbit/s, was installed between Europe (my team at CERN) and the Cornell node of the NSF network, in March 1990. Probably the two most significant events since 1990 were the release of the Mosaic web browser in 1993, and the privatisation of the NSFnet in 1995; these together enabled the public emergence of the Internet as the medium for business, entertainment and social interaction that it has become.

CC:: The Internet is a "network of millions of networks". Who owns the backbone of the Internet?

BC:: Although one often speaks of the "backbone" or the "core" of the Internet, there truly is no such thing. The network is structured as a mesh, with surprisingly little hierarchy. One can think of it as a very large experiment in graph theory, with the added twist that nodes of the graph have minds of their own and may misbehave in various ways.

In as far as there is a hierarchy, it consists of local Internet Service Providers (ISPs) offering packet-level connectivity to individual subscribers and to enterprises, and upper-layer ISPs offering national and international interconnections. Another component of the mesh consists of Internet Exchange Points (IXPs) which act as neutral packet exchanges. All of the players - local and upper-layer ISPs, IXPs, and enterprise networks - design their own network to provide the degree of redundancy they are willing to pay for.

Thus one can see that the "backbone" of the Internet, which is really a mesh of meshes, has no single ownership - it's a giant co-operative. This co-operative works because it is mediated technically by the routing protocol known as Border Gateway Protocol 4 (BGP4) and economically by business agreements between the ISPs - some of which are financial arrangements in which one ISP pays another for service, and some of which are peer-to-peer agreements to exchange traffic with no financial consequence.

The essence of packet switching using a protocol such as BGP4 is that when there is a breakage in the network for any reason whatever (natural disaster, man-made disaster, technical error, or even bankruptcy), the routing system will automatically reconfigure itself to avoid the damage. Thus there *appears* to be a stable core but the reality is otherwise.

CC:: How many ISPs deal with international interconnections? Are they pri-

vate or government-sponsored?

BC:: I can't really answer numerically, but the typical pattern in a country of any size is that there are some purely local ISPs who only handle local customers, and therefore buy their international transit service from a larger ISP with direct international connections. These larger ISPs will also have their own local customers. It's pretty rare today for international connections to be government sponsored - presumably that happens in a few countries, but private enterprise rules the roost. There is a handful of major international ISPs who operate more or less on a global basis. It's ironic that the Internet, widely used as a communications medium by anti-globalisation campaigners, is itself the epitome of globalised free enterprise.

CC:: The construction in 1985 by NSF of a university 56 kilobit/second network backbone was followed by a higher-speed 1.5 megabit/second backbone—the NSFNet. The transition from academia to more commercial interests began in 1988. In spite of the fact that nobody is in charge of the Internet, it seems that there is a strong link, from the very first days, between the USA government and the Internet. Is it true, and if yes, in which form?

BC:: Certainly at its origin, the Internet was mainly funded by the USA through the Department of Defence, but as a research project; it was never used operationally for military purposes. Even the early international extensions to Norway and the UK, which were funded under NATO auspices, were pure research exercises. The switch to NSF funding really marked the recognition in the US that the Internet was of general utility to the scientific research community (i.e., networking *for* research instead of research *about* networking). A similar pattern applied as the Internet grew in other countries, although in many cases the motive for government funding was the support of research *and* education; hence the designation NREN (National Research and Education Network) that is often used. For example, the growth of government or university funded NRENs in Eastern Europe after the fall of communism was spectacular.

When the NSFnet was closed in favour of commercial ISPs in 1995, two things happened. One was that a group of US universities created the Internet2 project, effectively a high-speed NREN for the USA. The other thing was that key administrative functions of the Internet, previously funded under contract by the US Government, had to be housed somewhere. There was much discussion of what to do, revolving around the late Jon Postel, who had been running those administrative functions for many years. (I was chairing the Internet Architecture Board at that time, and thus found myself in a meeting in the Old Executive Office Building in Washington DC with Ira Magaziner, who was working on this issue for the Clinton/Gore Administration.) The result, considerably simplified, was that an independent not-for-profit corporation (ICANN, the Internet Corporation for Assigned Names and Numbers, see `http://www.icann.org`) was created to take

over this administrative work. In the creation of ICANN, there was a triangular tension between commercial interests (who wanted a free-for-all), governmental interests (who saw the network as an emerging national asset), and the general Internet community (who saw the network as a worldwide communal asset). At the end of the discussion, and under heavy pressure from the US Government, ICANN was set up independently, but operating under US laws and under an agreement signed with the US Department of Commerce. This was a compromise, and like any compromise is disliked by some. As we speak, discussions about termination of this agreement are proceeding, with the same triangle of interests still evident. However, the Internet's administrative functions have continued without a break, from the beginning of the ARPANET until the present day.

BC:: (2014) In early 2014, the US Department of Commerce announced its intention to end its contract with ICANN, leading to vigorous discussion in the Internet governance community. We can come back to that later, because it has interesting ramifications.

CC:: I tried to read more about the Internet2 project and found quite a wealth of information at `http://www.uazone.org/znews/internet2/internet2.html#Internet2`. In particular, there seems to be a mixture of projects going under the Internet2 umbrella, some sponsored by NSF, some by a consortium of universities, while others are funded by the USA Government. The project includes also Canada and some European partners as well.

BC:: Yes. It's an important project, even though its name is a little confusing - it is a major R&D project that also provides services to US academia, and as you say it collaborates widely with other regions. We could also mention the many projects in networking sponsored by the European Union's R&D Framework Programmes, and similar projects in the major Asian economies. Generally speaking there is strong synergy between the NRENs and national or international R&D activities, continuing the trend set by the ARPANET forty years ago.

CC:: Are there basic goals for the development of the Internet?

BC:: There are so many special interests today that there must be a hundred answers to that question, depending on who you ask. My personal opinion is "the three S's": scaling, stability, security. We need the Internet to scale up to support a human population of ten billion people. We need it to be stable and reliable. We need it to be secure, both to protect privacy and freedom of information, and to minimise abuse.

CC:: Who pays for the Internet?

BC:: You do, Cris! In general, the network is user-funded (whether the user in question is a private individual, a business, or a research or education institute). Obviously in some cases the funds come ultimately from taxpayers, but outright government subsidy is rare.

CC:: Is anybody (organisation) theoretically capable of shutting-down the In-

ternet?

BC:: I don't believe so, although the difference between theory and practice is hard to define in this case. In what one might call theoretical theory, ICANN could instruct the operators of the thirteen "root servers" of the Domain Name System (DNS) to cease operations; if they obeyed, nobody would be able to convert names to addresses any more. But on any realistic theory, some of those root server operators would simply refuse to obey, and only one of the thirteen is needed for the network to carry on.

There is always the risk of cyber-sabotage to the DNS or the basic world-wide routing system (the afore-mentioned BGP4). However, those systems were designed to be resilient against partial failures, which makes total failure under software attack most unlikely.

CC:: I like the syntagm "theoretical theory": it reminds me of Jaffe and Quinn "theoretical mathematics" (used in their provocative paper published in *Bull. Amer. Math. Soc.* 29 (1993), 1–13).

BC:: Well, Internet engineers have a saying: In theory, there's no difference between theory and practice, but in practice, there is!

CC:: Interestingly, we have thirteen "root servers" of the Domain Name System (DNS). Am I really wrong if I "theoretically" call them the "Internet core" (not backbone)? It would be interesting to know more about them: Where are they located? Who owns them? Do they communicate between themselves in a special way?

BC:: They are certainly crucial. Without them, users would be reduced to typing in numerical addresses. They are located in very secure buildings scattered around the world, and they are owned and operated by a variety of organisations, including Internet registries, NRENs, universities, and three US agencies. And by the way, although there is a technical limitation to thirteen root server addresses, there are actually many copies of some of the root servers, using an addressing trick called "anycast", whereby multiple computers are able to answer to the same numerical IP address. There is a nice map at `http://www.root-servers.org/`. Root servers all supply the same information, which is supplied at global level by ICANN, so no horizontal communication between them is required.

CC:: The Internet changes "in flight", to use one of your expressions. Given its huge size, how is it possible to be so robust?

BC:: Firstly, the basic principle of connectionless packet switching is that each packet travels independently of its colleagues, and includes its own source and destination address. This in itself turns out to be a strong point for robustness under change (whether the change is essential or accidental): we basically have only one atomic operation to perform - send the packet in the right direction.

Secondly, from the beginning it was accepted that packets may get lost or damaged. This led to the "end-to-end principle" of design (first documented by

Jerry Saltzer and colleagues at MIT). This states that the end systems in a communication should not assume any function inside the network *except* a best effort to deliver packets. All functions such as error detection, error correction, retransmission and security should be provided solely by the end systems.

Again, this principle is a very strong point for robustness - even if the network discards a noticeable fraction of the packets, end systems can and must recover the situation.

This principle hasn't been applied perfectly (firewalls are a counter-example) and cannot work perfectly (as glitches in Voice over IP calls show) but it has kept the Internet up and running since 1983.

CC:: What is the Internet Engineering Task Force (IETF, see `http://www.ietf.org`)?

BC:: It's the self-organised community that develops and maintains the basic standards for Internet protocols - the Internet Protocol (IP) itself, transport protocols (TCP and others), elementary application protocols, and associated routing, security and management protocols. Although the IETF grew out of the original ARPANET project, it is now completely autonomous, very international in nature, and largely populated by engineers from companies in the networking and IT industries. It's organised in about 120 separate working groups, and holds three week-long meetings per year. However, most of the detailed work is carried out by email, allowing effective remote participation. The IETF's distinguishing characteristic is that it has no formal membership and no voting - decisions are taken by arguing to the point of rough consensus.

CC:: There is a myriad of committees and organisations related to Internet standards (your webpage once listed more than 50 such organisations you were aware of). Do they have any impact?

BC:: Sometimes yes, sometimes no. We see cases of small industrial groupings creating a self-appointed "standards consortium" with quite expensive membership fees to develop a standard for a very specific technology. If the technology succeeds commercially, this rather closed "standard" can be very helpful to the companies involved (especially if the technology is patented). We also see cases of *ad hoc* consortia developing standards for a new general-purpose technology. If the consortium acts in an open manner and its technology succeeds in the market, everybody benefits. The IETF (founded 1986) is indeed an example of this. The World-Wide Web Consortium (founded 1994, see `http://www.w3.org`) is another. In general, it seems that a standards organisation that has open debates and modest fees, and embraces general-purpose technology, has more impact than one with closed meetings and high fees that deals with very specific technology.

CC:: "Spam, fraud, and denial-of-service attacks have become significant social and economic problems"—you recently wrote in your paper "Better, Faster, more Secure" (*Computer Architecture* 4/10 January 2007). Can we briefly discuss

all these three problems? Let's start with spam. A paper "Most spam comes from just six botnets" by John Leyden (posted at `http://www.theregister.co.uk/2008/02/29/botnet_spam_deluge`) claims that "Six botnets are responsible for 85 per cent of all spam, according to an analysis by net security firm Marshal". What's a botnet?

BC:: It's a large set of infected computers carrying a specific item of malware (malicious software), which acts collectively as a robot under the control of a *botmaster* who is a malicious individual. The infection is of course distributed like any modern virus, by infected email or web sites.

CC:: How does the scheme work?

BC:: Simple enough. The malware might be constructed to pull a number of email addresses at random from the infected host's email address book, and send a particular spam message to those addresses. The botmaster, who sells his services on a black market, will broadcast the spam to all his bots, using intermediate hops to obscure his true location. His bots will then send the spam onwards, from and to seemingly random addresses. (It isn't sexist to say "his"; these people always seem to be male.)

CC:: The six botnets refereed to by Leyden are well-known. Why is so difficult to fight them?

BC:: Firstly, botnets send spam and their own malware can be transmitted via infected spam. So the population of infected machines is self-propagating almost at the speed of light. Secondly, botmasters are hard to find, since they use intermediate hops as proxies. They *can* sometimes be found, as the example of the botmaster "AKILL" convicted in New Zealand showed.

CC:: Who benefits from the "genuine" garbage spam?

BC:: I think you mean spam that appears to have no coherent content in any language. Well, it could be a vector for infection. It could be practice for a botmaster, or a rather silly form of denial of service attack. Or maybe it's the Martians?

CC:: What about fraud? Is authentication an enemy of privacy?

BC:: Remember that authentication goes both ways. If I, as a customer, am connected to the genuine web site of my bank, I expect the bank to authenticate me, and then to keep my transaction private, just as I would if standing at the counter. The real problem is in the other direction. If I mistype one letter in my bank's URL, and a criminal has created a perfect clone of the bank's web site, whose only purpose is to extract my password from me, how do I know that I have reached a fraudulent web site? For that, I would need to use the bank's public key in some reverse authentication mode. Personally, I'd rather be sure of mutual authentication before I start worrying about privacy. Cloned web sites used without mutual authentication are probably one of the biggest dangers today.

CC:: How difficult is to check for a web site whether it has clones?

BC:: Quite hard. The creator of the clone will not advertise except in fraudulent emails. The clone's URL name will be chosen to look visually as much like the original as possible (perhaps substituting a "1" for an "i" for example), so that the victim is unlikely to notice. Another trick is to incorporate a common typing error in the fraudulent name, in the hope that a few people will visit the URL purely by accident. Ideally, of course, public key cryptography and trusted certification authorities suffice to verify that a "bank" is really a bank, but can we expect 100% of the general population to understand the subtleties of this?

CC:: What about denial-of-service attacks?

BC:: Unfortunately these are built into the packet switching model. If somebody chooses to send me an overwhelming flood of packets, the network does its job by delivering them. When a site is subject to such an attack, there are defensive techniques that can be used, but they are all palliatives - the rogue packets will continue to arrive. If they come from a single source, defence is relatively easy, and the source can be traced and blocked, but if the attack is launched by a botnet, defence is pretty tricky.

CC:: What is the Internet quality of service?

BC:: Traditionally, it's "best effort", i.e., packets will be delivered with high probability but not guaranteed. Some years ago when bandwidth was scarce, we could sometimes see apalling loss rates (up to 20% of packets lost) on congested routes; fortunately this is rare today.

There have been several attempts to improve on this, although in practice most ISPs simply tune their networks to minimise packet loss. The simplest solution to deploy is known as "differentiated services", in which packets are classified into a few classes of traffic as they enter the network, and the routers run a different queuing algorithm for each class of packets. For example, a very simple approach would be to put Voice over IP packets in a fast queue, and everything else in a best effort queue. As long as bandwidth remains cheap, this is probably all that is needed.

CC:: How can you measure it?

BC:: Traditionally one measures achieved throughput, loss rate, transit delay, and jitter. The first three will be means over a given period, and the jitter will express the variability of the transit delay. Throughput and loss rate are quite easy to measure using logging software at both ends; transit delay and jitter need synchronised clocks and driver-level software.

CC:: How safe is the Internet? Some problems are clearly not "technological": we cannot stop somebody to voluntarily give his credit card details to a phishing site, can we?

BC:: Exactly. But neither can we blame someone with poor eyesight for not noticing a mistyped URL, nor an ordinary consumer for failing to have fully up to date virus protection. However, I think it's hard to argue that the Internet is

really more dangerous than the rest of society; there have always been con-men, and there have always been victims.

CC:: Is Web 2.0 a meaningful concept?

BC:: It's certainly true that there seem to be a number of new, dynamic application layer technologies sitting on top of the old static web and the first generation of interactive mechanisms. I find it very hard to see a break point where we changed from Web to Web 2; perhaps I've been watching the standards and technology evolve for too long. I think the keyword is "evolve", because nobody can afford discontinuity if they're trying to run a business. The notion of a web site being "Closed for maintenance" is not even funny! So I think that Web 2.0 is a nice marketing name for routine progress.

BC:: (2014) The buzzword has changed since 2008: now the next new thing is HTML5. Again, it's really not much more than routine progress. But the problem caused by relying on new features when many users still run old browsers will only get worse.

CC:: What about a "parallel" Internet? Is it possible? Is it going to be safer? Is it feasible?

BC:: It's a delusion. Again, the Internet is a business now. Discontinuity just isn't an option. Anything new that comes along simply must plug into what we have. Of course, this doesn't preclude testing out new ideas on isolated test networks, but to be of real value, it must be deployed on the main Internet.

BC:: (2014) We'll talk about the Snowden revelations later. However, one political reaction they have produced is the notion of a European network so that traffic doesn't pass through America to be spyed upon. Again, it's a delusion. The Internet only has value because it's worldwide; and traffic can be spyed upon just as easily in Europe as in America. Similarly, attempts to limit Internet access to approved content, as some countries have tried to do, will ultimately fail. Where there's a will, there's a way round the filters.

CC:: Please tell us more about IPv6.

BC:: This is a case in point. The 1970's design of IP only allowed in theory for four billion addresses, and in practice we can't use them all. So we need a new version of IP, which because of a few false starts is version 6, allowing for an almost unlimited number of addresses. It's well defined and is included in many products now, but there are quite some practical challenges to get it into general use without discontinuity. This is must happen over the next few years, because otherwise the Internet's address registries are expected to run out of address space in about 2010. I think this is an area, like the early Internet, where universities should take the lead.

CC:: This is interesting, how "unlimited" is the number of addresses allowed by IPv6 and what is the reason for this huge jump?

BC:: The decision was taken to expand the address size of the old IPv4 pro-

tocol from 32 bits to 128 bits in IPv6, which raises the size of the address space to the fourth power, or increases it by 29 orders of magnitude, to about 3.4×10^{38} addresses. Obviously, nobody expects to address that many objects in the Internet. The reason for the large increase is to allow some structure within an address, for example to allow separate parts of the address to represent a particular subnetwork and a particular computer interface on that subnetwork.

CC:: You have been heavily involved in the design of IPv6—your talk on this topic given at IBM in Auckland a couple of years ago steered my interest in data communications. Please tell us more about your own contributions to the project IPv6.

BC:: I was fortunate enough to become an active participant in the IETF just when its study of "IP - the Next Generation", or IPng, was starting, in 1993. We considered several alternative proposals and finally a rough consensus was formed for what became IPv6. I helped in the analysis and comparison of those proposals, and I've been contributing to the standards development process ever since. Actually the basic IPv6 standard has hardly changed since 1996, although there has been constant tuning and refinement. What has proved very hard is developing operational solutions for the co-existence of old IPv4 and new IPv6 during the transition process. It's been described as attempting to change the engines on an aircraft in flight. Among other things, Keith Moore (University of Tennessee) and I contributed one of the mechanisms for connecting IPv6 "islands" together across an IPv4 ocean. Altogether, I've contributed substantially to numerous IETF "Request For Comment" documents on IPv6 topics. Today, I'm most interested in practical deployment issues.

CC:: I know that predictions are hard, but I cannot resist asking you the obvious question: "What's coming next?"

BC:: I hoped you weren't going to ask that. I certainly hope to see IPv6 in general use by about 2015 (five years later than my original hope). There will need to be some changes in the wide-area routing system to cope with continued growth, and active research is going on in that area. I hope we see security functions moving to their proper place in the end systems, with the role of firewalls declining. I think we'll see voice and video services in widespread use, although I doubt we will see the end of broadcast radio and TV. I'm sure that business use of distributed computing services will continue to grow. I'm really unsure what to expect in mobile services. Personally I find it hard to believe that the things I do on my PC or watch on my TV will ever translate to a hand-held device with a tiny keyboard. Two things that are pretty certain, however, are that everything interesting will run over IP, and that we will be surprised and delighted by new, creative uses of this wonderful infrastructure.

BC:: (2014) We are seeing decent growth in IPv6 now. The central registry (IANA) did indeed run out of IPv4 addresses in 2011, and the regional registries

are now approaching the same point. As a result, content providers such as Akamai, Facebook and Google are reporting rapid growth in IPv6 traffic. All the same, many content providers and Internet service providers still have work to do.

CC:: (2014) We've been reading a lot recently about Internet governance. What does that mean exactly?

BC:: If you ask that question to ten people, you will probably get ten different answers, so I can only give a personal opinion. There are many aspects of Internet technology that need to be specified, administered and operated in a way that is really just a technical matter that doesn't deserve the term "governance." Also, there are many societal impacts of modern telecommunications that do require some kind of governance but are not specific to the Internet - essentially these are the effects on society that Marshall McLuhan predicted as effects of electrical communication long before the Internet was invented. These issues aren't contingent on the Internet as such, and society needs to deal with them regardless of Internet technology. Examples are freedom of information, privacy of personal information, consumer protection, electronic fraud, and so on. However, between these very broad issues and the purely technical aspects of the Internet lie a number of issues of societal importance that are directly linked to specific aspects of Internet technology. These, in my opinion, are the proper subject matter for the discussion of Internet governance.

The problem we have is that, too often, the very broad societal issues are lumped together with both Internet governance issues and even some technical issues. This leads to very confused discussions and to false conclusions. A good example is pervasive surveillance, which we should also discuss.

CC:: (2014) Which topics, in your view, really fit into the Internet governance rubric? And where should the other topics be discussed?

BC:: I have quite a short list of Internet governance topics:

- The creation of new top level domains in the DNS.
- The resolution of disputes about names within top level domains.
- Privacy of registration data.
- Interconnection arrangements between ISPs.
- Coordination of security incidents with law enforcement.
- Tracking and tracing domain names and IP addresses across national borders for law enforcement purposes.

There may be others, but I apply a tight criterion: the issue needs to have societal impact and it needs to be contingent on specific Internet technology. Thus, for

example, I exclude spam, which can be delivered by multiple technologies, not just the Internet, so it should be covered by laws and treaties about fraud and consumer protection. Perhaps surprisingly, I also exclude network neutrality, because it is a competition and consumer protection issue. This exemplifies the answer for all the other topics. They are issues that society has to manage irrespective of the Internet, by social contract, law or treaty as the case may be.

CC:: (2014) What risks are there if the governance arrangements fail in some way?

BC:: Internet engineers have a saying: "The Internet routes around damage." Originally this referred to resilient routing algorithms, but it's turned out to be much more generally true. I suspect that if something went seriously wrong in the governance area, people in the technical community would rather quickly get together and cobble a new organisation into existence, on a volunteer basis, probably over the weekend. The people who end up in Internet operational jobs tend to be can-do people who react quickly under pressure.

CC:: (2014) You seem to be saying that pervasive surveillance isn't an Internet governance issue as such. Then whose problem is it?

BC:: It's fundamentally a political problem. For students of the history of signals intelligence, there is a very direct line between Room 40 at the Admiralty in London during World War I, Bletchley Park during World War II, the equivalent activities in the USA, and the widespread surveillance revealed by Edward Snowden. Since we're having this conversation in New Zealand, it's worth recalling that today's signals intelligence operation here (GCSB) is the direct descendant of New Zealand's cooperation with Australia, Canada, the USA and the UK during World War II. It's absolutely no surprise that these activities, which started as literal wire-tapping on telegraph cables, have been extended to cover mobile telephones and the Internet. Of course, the extent of the surveillance, and the way it can touch ordinary citizens, is new and has shocked many people. And the only safe assumption is that all major governments are doing this, not just the Americans and their English-speaking allies.

Technically, what's going to happen is that standards and software to make end-to-end encryption easier to use will appear over the next year or two. But secret key management is an enormous challenge, even for sophisticated organisations. How ordinary citizens can be expected to do this is beyond me. Citizens need to be able to trust their own government and, worse, other governments too. That's a challenge for the democratic process and the rule of law.

CC:: (2014) What about ICANN today? The US government has announced its intention to terminate the contract between the US Dept of Commerce and ICANN in 2015. Does this matter for global surveillance?

BC:: As mentioned earlier, ICANN is a not-for-profit corporation which basically has an administrative job - registering and publishing the parameters needed

by Internet protocols. But that has an aspect that borders on governance: what policies should apply for assigning valuable resources? Fortunately, most parameters aren't valuable, but some are: especially IPv4 addresses, which are scarce, and top-level domain names, such as *.com* and *.nz*, which have clear marketing or political value. It's mainly the policy aspects of the latter that have been contentious at ICANN, and it is the oversight of domain name policy that the US Government proposes to relinquish. In my view, there are several reasons why this has become a contentious question. Firstly, there is a great deal of money to be made out of registering individual names in popular domains like *.com*, so the right to operate such a registry is very valuable. Secondly, national domains like *.nz* have a political dimension, especially in countries with unstable politics. Thirdly, and most recently, domain names written in non-Latin scripts have a cultural and emotional power of their own.

But to answer your question: despite the contention about oversight of ICANN, nothing that ICANN does - all of which is fundamentally administrative in nature - has any effect on the ability of any government agency to spy on Internet traffic. The American agencies accused of breaching the privacy of others in this way aren't connected to the Department of Commerce, and in any case would have nothing to gain by interfering in the administration of Internet names, addresses or protocol parameters. And of course there is every reason to believe that many other governments also conduct such surveillance, at home and abroad.

CC:: (2014) The NSA "persuaded" web-encryption company RSA to develop a "more vulnerable" random number generator. RSA said it should "have been more sceptical of NSA's intentions". In fact, any pseudo-random number generator is provably weak, so why are these methods still in use?

BC:: I'm not a cryptographer, but in any case I suspect that the answer lies in economics (an equally black art). Asymmetric cryptography is computationally expensive. Efficient encryption and decryption needs some kind of shared secret that a third party finds unreasonably expensive to guess, both now and reasonably far into the future. I suspect the answer to your question is that for most purposes, the cost of a successful guess, even with a weak PRNG, far exceeds its value. Of course, the NSA is one of the few organisations in the world that we can assume is prepared to pay a very high cost to make a successful guess once in a while.

Also, as our colleague Peter Gutmann has pointed out, the vast majority of known security breaches (including ones known to have been made by the NSA) worked by bypassing encryption. That turns out to be much, much easier than cryptanalysis.

CC:: (2014) Sir Tim Berners-Lee has marked the 25th anniversary of WWW (12 March 2014) by calling for a Magna Carta bill of rights to protect its users. Would this help in freeing the internet from governments meddling?

BC:: Every little helps. For example, in April 2014 a conference called NET-

mundial (or more formally, Global Multistakeholder Meeting on the Future of Internet Governance) took place in São Paulo, Brazil. It produced a sort of manifesto that goes in the direction Tim was talking about. In particular, it de-emphasises government inputs. However, a fact of life is that governments control what happens in their own countries, and that does include the Internet. So all Internet freedoms simultaneously depend on and enhance democracy and the rule of law. There is a good reason why reactionary regimes tend to dislike the Internet; it is indeed their enemy.

CC:: Many thanks.