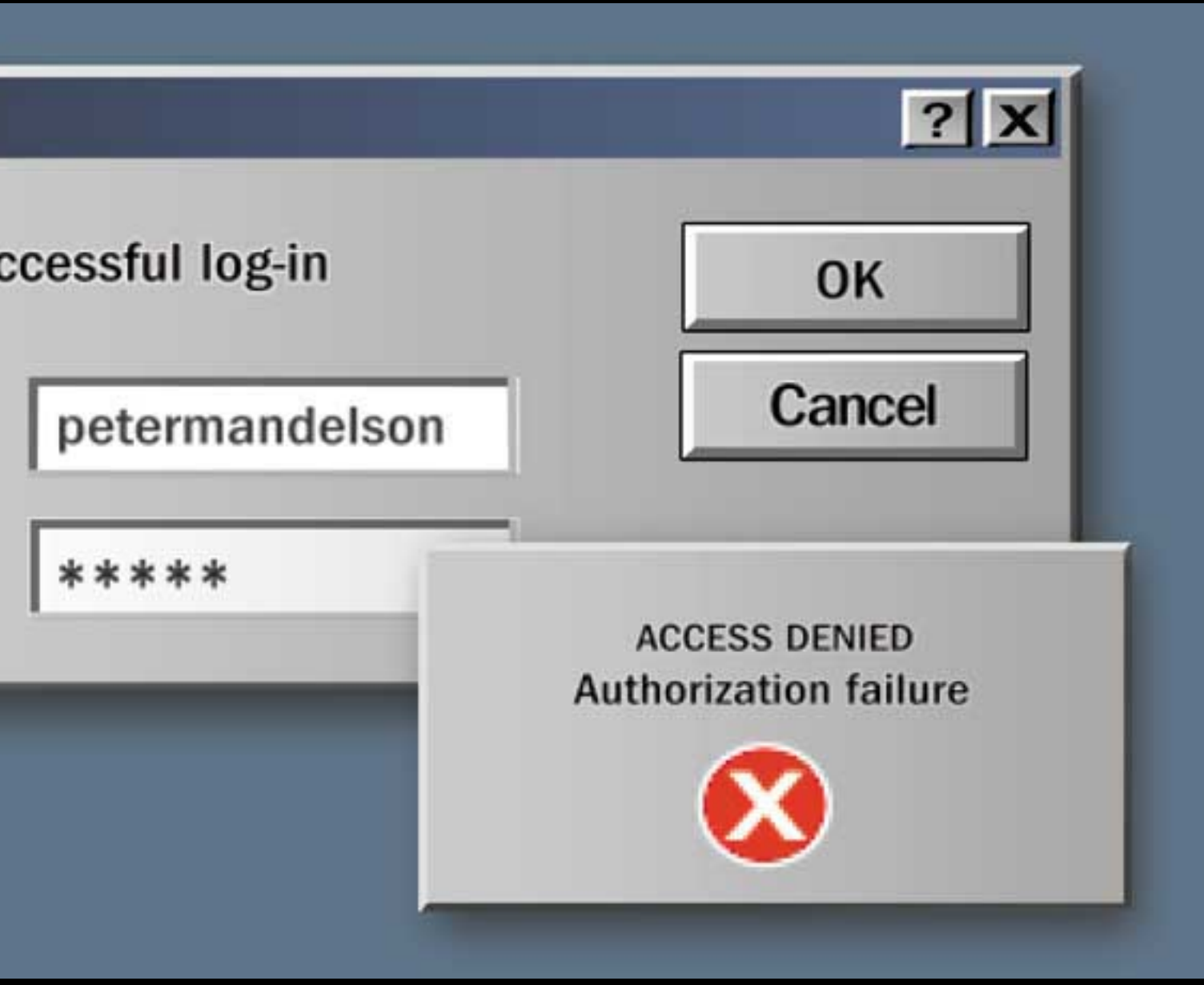
newstatesman

Special Supplement

# Internet Security



newstatesman NEW MEDIA AWARDS TWO THOUSAND AND THREE

# Safe surfing

Public confidence in making transactions and placing personal details on the internet remains low. In a recent survey conducted by the *New Statesman*, most people said they feel more comfortable using their credit card at a restaurant than online, and a significant number revealed they choose not to use the internet because of fears of fraud. Those who do enter personal data on the internet rarely read or understand website terms and conditions or privacy policies.

The public's worries over internet security are often misplaced. One example concerns the use of credit cards. Although credit card fraud is common on the web, it is rarely the result of an insecure site. Most incidents involve details stolen in the real world rather than via hacking. Individuals are more likely to become victims of credit card fraud by discarding a receipt than by using the net.

Consumers, businesses and the government stand to lose from this lack of confidence. The UK is in a strong position to excel in both e-government and e-commerce, but opportunities will be missed if concerns about security continue. Solutions that omit or limit the use of credit cards are already in place and have been eagerly taken up by consumers. These solutions vary, from using mobile phones to having online accounts, but many of these schemes are for small rather than large payments. Authentication services are being used more and more on UK websites. However, a number of questions arise from this, particularly regarding regulation. By its nature and origin, the internet is largely self-regulatory. If public fear about online transactions is to be overcome, there may need to be a more widely recognised "trust mark".

The following edited round-table discussion, part of the *New Statesman* New Media Awards 2003, examines some of the fears and considers how public confidence is to be increased.

**Kathryn Corrick, online manager**

## contents



Editor: Emily Mann Design: Leon Parks Cover: Dan Murrell
Research: Hannah Parham

newstatesman subscriber services: **Stephen Brasher**
Freephone: **0800 731 8496** E-mail: **sbrasher@newstatesman.co.uk**

Published by New Statesman Limited. A supplement to the newstatesman issue 22 September 2003.  Registered as a newspaper.
Address: New Statesman, 52 Grosvenor Gardens, London SW1W 0AU

# Round-table participants

**Charlotte Barrow** I'm project manager for the Cyperspace Research Unit at the University of Central Lancashire, which researches children's use of the internet.

**John Carr (chair)** I'm an IT consultant and work with children's organisations on internet safety issues. I'm a member of the Home Office's internet task force and the Department for Education and Skills' Internet Safety Strategy Group.

**Mike Galvin** I am director of internet operations at BT. I'm principally responsible for most of the retail infrastructure we provide, but also for security and law enforcement issues.

**Stefan Haselwimmer** I am the managing director of PhoneAnything, which is developing e-commerce systems for land-lines and mobiles.

**Detective Chief Superintendent Len Hynds** I am the head of the National Hi-Tech Crime Unit, part of the National Hi-Tech Crime Strategy. I also chair the Internet Crime Forum and the Association of Chief Police Officers' National Hi-Tech Crime Working Group.

**Scott Law** I am managing director of Metacharge, an e-payment service designed around the needs of digital content and service providers.

**Geoffrey Llewellyn** I am director of strategy and government relations for Schlumberger in the UK, and have been heavily involved in the entitlement or ID card debate.

**Simon Moores** I'm here from eGov monitor. I write about and consult on security, e-government and so on.

**Brian Neale** I manage the security consulting practice for Hewlett Packard Services in the UK.

**Andrew Pinder** I am the e-envoy. My job is to work from inside the government to promote information technology in the UK.

**Sandra Quinn** I am director of corporate communications at the Association for Payment Clearing Services (Apacs), which co-ordinates banks' activity on internet payments and fraud.

**Detective Sergeant Steve Santorelli** I am from the Computer Crime Unit at Scotland Yard.

**Paul Wood** I am chief information security analyst for MessageLabs, an internet security company that specialises in scanning e-mail for viruses, spam and other unwanted content.

# Confidence in internet security

## Round-table discussion

**John Carr (chair)**
There is a sense of worry about the internet, particularly as a medium for conducting business. Even though you are much more likely to have your credit card ripped off by a waiter at the back of a restaurant than you are by doing any kind of online transaction, that is not what the public appears to believe.

**Andrew Pinder**
The paranoia about the internet is partly a result of the media. What I have been trying to get back into the debate is some sense of proportion and how likely certain things are to happen. Let's be sensible about things.

Having said that, there are some genuine issues to debate, such as what technologies we need to employ to protect people on the internet and protect their transactions. Government has a role in trying to make sure that something is done somewhere. It has a role in providing support for those who want to do something (whether that be financial institutions, internet service providers or government itself) to deal with the problem and make people feel safe using the internet – so they are sensible, but not paranoid.

**John Carr**
I was recently in Australia listening to a very learned professor who is an adviser on internet security to the American Federal Trade Commission. One point he made with some force was that, while the primary responsibility of companies is to make a profit and keep their shareholders happy, and they would invest in security systems to help achieve that, he wasn't convinced they would put in extra effort and investment to achieve the level of security that would make society in general feel more confident. In other words, he

suggested that there was some distance between corporate interests and what wider society – represented by the government – might think was reasonable.

**Simon Moores**
Putting it simply, you could say that industry is unable to inspire confidence, and certainly government is unable to offer leadership. As a consequence, the people out there using the internet don't know which way to turn. We are arguably back where we were three years ago. People don't believe that the internet offers them an environment of trust, and they don't believe that the industry in the shape of the vendors, whether it be Microsoft or anybody else, can deliver the solutions that might provide that environment of trust.

**Geoffrey Llewellyn**
This is a classic argument about the public good. The government really does need to create the environment of trust and the set of parameters within which the private and voluntary sectors can work. I wouldn't be quite so scathing about the past three years, but I do think the government faces a major communication challenge at the moment.

**Mike Galvin**
In the time I have been involved in the internet, I've seen the opportunities in terms of e-commerce and reaching people's lives, and also the threats to people's freedom and things like spam, come more and more to the fore.

> We don't fully understand what the opportunities and threats are. They are not mature yet in this industry

We don't fully understand what the opportunities and the threats are. They are not mature yet in this industry. For example, conversations we are having about threats today are not the conversations we were having 12 months ago. Hitting this moving target is going to be very difficult, whether with legislation, industry action or technology.

**Andrew Pinder**
Things are actually a lot better than they were three years ago. There's a lot more e-commerce happening on the internet. All our surveys say that people are more confident about using the net than they were three years ago. More people are doing a lot more transactions online, and we are not seeing significantly increased fraud.

Yes, government and industry can do some things, but only if people are prepared to pay for it. How many people, if they were asked to pay extra for having their e-mails scanned, would actually pay? Let's stop saying "there's no leadership, it's all terrible, it's far worse than it was". There needs to be a proper debate about what should be done. To throw everything back into the lap of the government and say, "Until government does something, it isn't going to get any better" – that's a load of cobblers.

**Geoffrey Llewellyn**
I'm not saying that nothing has been done or that there

has been no achievement, but there is an opportunity for the government to provide more effective leadership. It isn't communicating sufficiently.

**Andrew Pinder**
I do take issue with that. There clearly is a communication issue, but one of the things the government faces is hysteria in the press, pushed along by people who have vested interests in creating hysteria – the specialists in security, the firms who push security, who want to create a fear that will create customers – and I find sometimes that it is just impossible to fight against that sort of tide. Until you can have a rational debate, and talk about the real issues as opposed to simple and wrong assertions, you can't actually deal with the problem.

**Steve Santorelli**
The media sensationalises hacking attacks. If you ask people why they don't want to shop on the internet, they are concerned that their credit card details and so on are going to be intercepted in transit. In reality, this is very unlikely to happen.

The problems are twofold in my experience. First, there is the aggregation of credit card information in databases attached to the web portal itself, which means that when you go back to a site it remembers your card details. That is a magnet for hackers, who can break in through a web portal and get hold of the database. The other real problem is social engineering attacks: we see an awful lot of spam e-mails.

New users must be educated so that they understand the risks. The problem is, although it won't cost a huge amount of money to educate people, education will identify some of the vulnerabilities, and industry doesn't see that as beneficial to e-commerce. Industry doesn't necessarily want to highlight the dangers because doing so is likely to turn customers off and make them less likely to return to that particular site.

> The government faces hysteria in the press, pushed along by people with vested interests

**Simon Moores**
On the issue of confidence and the government's ability to react, let's think about broadband. We are doing quite well at broadband. A lot of people are now connected to broadband, but more than a year ago concerns were expressed about its security. The research, the information warning the public about broadband and about the steps they should be taking, came a year late. It suggests to me that the government was very concerned about promoting broadband first and worrying about the security issues later.

**Paul Wood**
I work for one of the internet security companies that Andrew thinks are contributing to the paranoia. In the past couple of months, I think there has been an increase in viruses and spam, especially through broadband. Our surveys show that home users are the worst for disseminating viruses. They don't keep their anti-virus signatures up to date. They don't have the right firewall-type software installed, so businesses that tend to deal with home users are at the greatest risk at the moment. Certainly, there isn't enough education or understanding among home users of what the new threats emerging in the past two months or so actually are.

I think the onus is largely on the internet service providers (ISPs) to ensure that the traffic and services on their networks are not compromised. It's difficult to say that they have to scan e-mails and things like that because there is a cost, and a number of ISPs are finding it difficult to turn in a profit at the moment. But they certainly should have a responsibility to protect their users in terms of what they are putting on their own machines.

**Mike Galvin**
I hear what's been said around the table about widespread concern over using the internet, but when I look at our customers' traffic I see a completely different picture. I see more people spending more hours online, and that trend has been almost universal over the past five to six years. There is some concern in some quarters, but the main problem is ignorance.

In spite of attempts to educate users, I think they are largely unaware of the dangers when they go on the internet. There are between 20,000 and 30,000 new broadband customers across the UK every week, so you are fighting very much a losing battle in the education stakes, but education is the key thing for us.

**Steve Santorelli**
If I had ten seconds to speak to every home broadband user in the country, I would tell them to get some anti-virus software and update it, and I would tell them to get a hardware or software firewall. When people phone us and say that something strange has happened, they've

**ns survey**

Almost half said they do not use the internet for shopping; the majority use the web for information and entertainment

**ns survey**

21 per cent said they would not consider shopping online; around one-third of those who do not shop online are dissuaded because of fears over security and fraud

been hacked or whatever, and we ask what firewall or anti-virus software they're running, the majority say that nobody has ever told them what software they should have on their systems.

Broadband has taken off in this country in a way that I never thought it would. It's a great opportunity. But whose responsibility should it be to educate the home broadband user? Should it be the PC manufacturers' problem? Should it be the ISPs' problem? There is an argument that the ISPs have an opportunity – rather than an obligation – to assist the government with the education of this army of home broadband users.

**Paul Wood**

We've talked about the home user market, where there's certainly a very great risk. But recently, while researching a story on spam, I found that a major international airline didn't have the right security in place. The size of the problem means it would be very difficult to solve through any legislative framework.

**Len Hynds**

What we have to do is see the problem for what it really is. It's not just about interdiction by law enforcement across a whole range of crimes. It's about understanding the problem and co-ordinating a response, and then informing the public and industry in a measured way so that they really understand. They don't want the hype, but nor do they want things to be played down. We have to find the middle ground and work together on it.

> Let's start by trying to work out what our priorities are, and who should be doing what

**Andrew Pinder**

I agree with that. What I really want is a rational conversation – a bit like this one – which says there is a problem, there are multiple problems. There is financial fraud, there is spam, there is pornography, there's child abuse, there are technology issues – a whole range of things that get in the way of the system working and which we want to tackle. But let's start by trying to work out what our priorities are, and who should be doing what.

I recently acquired a new role in addition to that of e-envoy, which is the central sponsor for information assurance in the UK. We are still trying to work out what the hell that means. We have produced a strategy for information assurance for the UK. A part of getting that document together was understanding what the priorities are and where the parameters lie. We want to try to engage in a proper debate because there really are problems. Spam is a particular problem at the moment, and I suffer from it more than most because, for fairly obvious reasons, people put my e-mail address on spam lists and so I get mountains of the stuff. There clearly is a big problem. We want to try and tackle it. It is a co-operative effort, but it is not helped by the noise and hysteria around it.

**Stefan Haselwimmer**

We were talking about promoting trust on the internet.

If someone's house is broken into, they know whom to contact to report it. If someone receives a virus, all they have to consult is the private company that provides their internet connection. There's no body in government for people to go to, or to which we can look for leadership on this issue.

**John Carr**
It doesn't exist yet, but it is being actively pursued, and BT is involved in developing a proposal for a one-stop shop. It was mainly the police who raised it in the first place.

**Len Hynds**
There have actually been three pieces of work in relation to developing a single portal through which these kinds of incidents could be reported. The one-stop shop was examined in two working groups, which have now been brought together. They are looking at providing a single interface to deal with a whole range of problems that people can encounter on the internet. I entirely agree that it is unacceptable that somebody should have a problem and have to come offline and then phone around trying to find the answer to that problem.

One concern we have to address in developing such a portal is that, if you make it possible for people to report online, they are going to use the opportunity to report a whole range of different problems, and we have to be able to cope with that.

**John Carr**
Going back to what Mike Galvin was saying about internet security being a moving target, that's another way of industry saying leave us alone, we are not going to deal with this problem today because we know it won't be the same problem tomorrow. It seems to me that the industry is saying to the rest of us, including government, that it is not just about government, that it's all very difficult, it's all very technical, it's all very complicated – trust us, we know this much better than you do. It has become part of the standard ethos that self-regulation has to be the best way.

And one does begin to wonder whether we should be slightly more aggressive and slightly more demanding of the industry, and not just sit back and accept that it's all too difficult and it's all too complex. Maybe we are too easily fooled into thinking that it is as hard as they claim it to be.

> Should we not be slightly more aggressive and more demanding of the industry?

**Simon Moores**
I think the evidence is that industry is trying very hard. I've been looking quite closely at Microsoft recently and I know it is putting a huge amount of effort into removing the problems we have experienced in the past with the operating systems that it is going to be driving out tomorrow.

But one of the problems that we have is encouraging people to upgrade to more advanced versions that are less vulnerable. It is going to be three to five years, I think, before we have an environment that is even

**ns survey**

The majority who shop online do so for reasons of convenience; none do so because they think it more secure. Some think that goods are cheaper online, but very few think there is more choice

remotely close to one which can be secured in a way we would like.

**Steve Santorelli**
I don't think it is fair to require ISPs to respond to this on their own. So whose problem is it? A useful analogy here is the invention of the car. Car crime has been a problem for a number of years, and security is a factor in the way cars are designed and a factor we take into consideration when purchasing a car. But if your car gets broken into, you don't then sue the manufacturer or the person who cut the key for the lock. Cars became more secure through the 1980s and 1990s because that is what the market required. The government led that change along with the industry and the insurance companies.

So, for the internet, I think it is a question of the government showing the way but industry being required by the market – by the users of the internet – to make things more secure. I think it is very much a problem for society as a whole rather than just software or hardware manufacturers or ISPs.

**Geoffrey Llewellyn**
We are poised on the brink of a transformation of the productive potential of our economy and our society that is not unlike what happened in the Middle Ages when paper money, notes of credit and so on replaced gold being shunted around the world in large quantities. I think the upsides are just as huge as they were for the introduction of paper money and, latterly, for credit cards.

I think the corollary of that is you must have the equivalent of the mint, the equivalent of banks that recognise the authority of a central bank, and you must have mechanisms for international exchange that share the same language of financial exchange and financial probity. I think, therefore, that government has a role to ensure that those institutions are in place. Government needs to take an educational role, a communication role, a regulatory role.

**John Carr**
But clearly not a single national government. New means have to be found, whether it's through the G8 initially or whatever.

**Geoffrey Llewellyn**
Like we have, to all practical purposes, a global dollar economy, we have a global internet, and we recognise that it is not possible for the internet to be regulated by individual national governments. Instead of throwing up our hands in horror and saying, oh, it will never work, there needs to be international, multinational co-operation. The danger at the moment is that bad internet transactions, and bad stories about the nature of transactions, could drive out the good, and the way to get around that is with a regulatory environment.

It is very much a problem for society as a whole rather than just software or hardware manufacturers or ISPs

**Brian Neale**
One of my concerns is the balance between what we do

in security and what we do in terms of business functionality and cost and so on. We have to look at putting security and compromise in the same sentence. Individual users should be educated that there is a certain irreducible level of risk. There are technical things we can do, there is always a little bit more we can do, but we reach the point when we actually start to interfere with the reason why people are using the internet in the first place, which is about flexibility and freedom and liberty to do things.

To pick up on what Simon said about Microsoft working very hard to introduce new security mechanisms into their operating systems, when stories about that came out in the press, there was an immediate outcry that this is the way Microsoft is going to police the world, that nobody will be able to do anything without Bill Gates's permission – an over-reaction, perhaps, but there is a balance that we have to strike. Perhaps we should spend a little more time teaching people the equivalent of the Green Cross Code for using the internet.

**John Carr**
We may well end up with several internets. We've already seen the development of internet II and private networks being established by big global corporations. So we could end up with the internet as we know it being the place where loonies and poor people go, and a set of alternative networks with a level of security and certainty where the irreducible risk is even smaller than it is today. That may be a good or a bad thing, but I think it is already an observable trend.

**Simon Moores**
Splitting the internet into two different types was something raised by Lawrence Lessig from Stanford University years ago. I wouldn't be surprised if the Islamic world, over the next five years, created a walled garden because of security concerns and concerns regarding the internet as a western device. There are aspects of our culture that others do not wish to adopt, and also, in the light of what has happened over the past six months, they don't want the Americans peering over their shoulders.

**Stefan Haselwimmer**
I think the danger is that one looks to a technical fix for these problems when what you really need is people having confidence and a circumspect approach to using the internet.

If you take viruses, for example, people are constantly told not to open attachments, and yet they still do. You can avoid viruses in large part by not opening attachments unless you are absolutely sure who they are from. What happens is that people become overly confident in their virus protection, and then a new virus comes out and their computer becomes infected. I think the key is to make people understand the nature of the problem and be more careful. I don't think any technical fix will guarantee 100 per cent protection.

> The danger is that one looks to a technical fix when what you really need is people being circumspect

**John Carr**
A question we all need to bear in mind is: what if we somehow collectively fail to achieve this new level of awareness that everybody agrees is desirable? Should we

**ns survey**

One-third said they would not be confident using their credit cards online; 70 per cent said they would feel safer using their credit card at a restaurant than online

## ns survey

Almost half said that a security policy increases their trust in a website; 20 per cent said a previous positive experience makes them feel more confident

be content – should the government be content – to sit back and say, well, there you are, that'll lead to another outburst of spam, that'll lead to another crash in the critical infrastructure. Or should we be saying, no, this is a matter of the public good; there are certain elements of society increasingly dependent on this technology and we cannot allow this persistent failure to achieve new levels of awareness to become a constant impediment or obstacle.

**Andrew Pinder**
I absolutely agree with that. The government has to say that we are a society that is increasingly dependent on the internet, and if the internet goes down, or it is so unsafe as to make it unusable, that is a huge issue for us.

**Paul Wood**
Among our customers at the moment, there seems to be quite a low level of adoption of digital signatures and encryption-type standards. I just wondered whether people thought a drive for privacy would take on board more of a standard for encryption, but how that would then obfuscate law enforcement and monitoring of the kind of things that we are concerned with at the moment.

**John Carr**
I think the role of encryption is quite clear; it has got immense potential, immense value for protecting transactions. We heard at the beginning that it is not the transaction itself that is the real problem, but the storage of data. Maybe banks and credit card companies should be required to use strong encryption if they are going to store large amounts of personal information on their servers.

> We must understand the harm that encryption can be put to, and have a remedy for it

The concomitant of that is, because the bad guys will get their hands on encryption as well, industry needs to find more and better ways of helping law enforcement to crack it – obviously on the production of an appropriate warrant. It would not be right simply to carry on getting more and stronger encryption without understanding the harm it can be put to and having a remedy for it.

**Geoffrey Llewellyn**
The current data protection legislation was introduced when both the public's understanding and computer systems were much less sophisticated than they are now. It seems to me that there is a pressing need for the data protection legislation to be updated for the 21st century.

**Andrew Pinder**
I agree with that actually. Data protection legislation is not wrong, it just needs to take account of increasing technology, increasing ways of using the information. However, I think some of the greatest inhibitions to joining up government data are rooted not in the data protection legislation itself, but in individual pieces of legislation around particular transactions within government. So it is a rather more complicated task than simply taking the Data Protection Act and updating it. And there is a very delicate debate to be had about the trade-offs between giving people better service by joining up data that is held within government (it is by

no means capable of doing that effectively now) and people's genuine concerns about privacy.

I favour a voluntary approach that allows people like me, proving who I am, to opt in to allowing some of my data – but only the data I choose – to be joined up around government in order to deliver me a better service. But I can quite understand that some people would not want to go down that route. I think people should have the option.

**John Carr**

On the issue of privacy, something that particularly concerns us is children's welfare and safety online. People behave badly; people behave more badly if they think there is less chance of being caught doing it. So if you want people to behave better in the online world, you have to find more and better ways of convincing them that they are going to be traceable. And indeed, it has always been the policy of British internet service providers to make online transactions more easily traced. But as far as I can see, virtually nothing has been done to make that a reality.

The simple point I want to get across is that I am all in favour of privacy, and one can respect that people have the right to anonymity under certain circumstances. But if you preserve in all cases the right to be anonymous, and effectively to deceive people about who you are, it seems to me that anything we might want to achieve in terms of greater certainty about online transactions is always going to be an illusion. There has to be some way, in other words, of reconciling people's need to be anonymous sometimes with our communal right to have greater certainty about what is happening online all of the time.

**Andrew Pinder**

That is the classic dilemma for law-makers and policemen – the balancing of individual liberty against the need to protect other people – and what one is looking for is a middle ground so that in appropriate circumstances (and clearly the area of child abuse is one) you can trace and arrest wrongdoers.

**Simon Moores**

In respect of child abuse and other areas, legislation represents a sanction, not a solution. There will always be people who will modify their behaviour to adjust to the latest environment, and I think it is very important that the police be given the armoury and the tools, through legislation, to be able to pursue these people. But I don't think this is the solution; rather, the solution appears to be a technical one.

> Balancing individual liberty against the need to protect other people is a classic dilemma

**Andrew Pinder**

I think we are getting on to the issue of online authentication – how do I really know that it is really you at the other end of the dialogue I am having? I think we feel the voluntary regulatory approach, which is called tScheme, with digital certificates and so on, has simply not taken off in this country, and therefore we are probably going to have to do something a bit different. Clearly, one of the ways forward is for

**ns survey**

Almost half of online shoppers do not read security and privacy policies before making a purchase

there to be an increase in authentication techniques for those people who want to authenticate themselves, and for the rest of us to deal only with people who are authenticated.

**Scott Law**
I don't think that any of the issues we are talking about here have technology solutions, Technology can play a role, but we are never going to have a homogeneous environment – we can't press a magic button and upgrade everybody to the latest firewall or whatever.

As for encryption, it is much more frequently used to transmit data than it is to store data. It is unknown in my experience for a credit card to be transmitted unencrypted over the internet. But some merchants want to store data for the convenience of the consumer, so that you can go shopping without re-entering all your details. That is where there is a great opportunity for the government to work with industry to target a particular issue, as opposed to legislating around it.

> In two years' time, everyone will probably have cards with chips in them that will be pin-enabled

**John Carr**
Wouldn't it be relatively simple to say – I am being slightly provocative here, but it would require just one clause in a bill – if you store people's financial data, then the transmission bit is not the issue. If you store it on your servers, you have to store it in a secure form and it is simply not acceptable to store data in an unsafe way.

**Sandra Quinn**
I think practically everybody around the table has at one stage mentioned the word "education", which is key. There are merchants dealing in an online environment who really don't know how they should be managing this process. We are in the process of developing guidelines for those merchants.

The data storage issue is central. A number of calls I get fall into two categories: there are the customers who say they have been dealing with an online shop for a long time but they are getting increasingly worried that they are no longer asked for their credit card details, because the shop is already keeping them; and then there are other people asking, "If I have already told them this, why do I have to tell them again?". And so we demand an incredible balance as customers. We need to know the businesses we deal with that store securely, and those that don't, so we can make a consumer choice.

**Charlotte Barrow**
We deal a lot in the area of safer storage. I know there is no legislation at the moment to regulate how companies store credit card details, but Visa and MasterCard are making significant inroads to that.

**Sandra Quinn**
I think that, in two years' time, everybody around this table will have credit and debit cards with chips in them that will be pin-enabled. Instead of signing, we will be using a pin instead. When you have critical mass, when everybody has one of those cards, the actual devices that we need to slot into our PCs or our mobile phones to make that link will be easy and extremely cheap. You can almost imagine them being given away in boxes of cornflakes.

**Andrew Pinder**
A big problem here is that I don't think these cards would be strongly enough authenticated at the issue point. How do you get that card in the right hands and make sure it stays there? It is the whole authentication process, rather than just the device itself, which is critical.

**John Carr**
In the debates on national identity cards, a scheme that has potential for online authentication, is there any discussion about having some kind of biometric element to it, and for it to be used extensively in the online world? It seems an obvious thing for us to want to see happen.

**Andrew Pinder**
I guess that, if at any point in the future a national identity card was introduced, then an obvious advantage of it would be making sure – assuming it was a securely issued card – that it could be used for e-government and perhaps other transactions. But we are not there yet and I think it will be a while before we are there.

**Geoffrey Llewellyn**
I feel that the key to making an ID card, an entitlement card or an enablement card – a strong authentication – does lie through biometrics.

**Sandra Quinn**
I think there is a real difficulty about the use of biometrics. Millions of us have credit and debit cards, each of us on average has three, so what you are looking at is a mass-produced product. To get biometrics on that level is just not a viable option.

**Andrew Pinder**
The problem is not of logistics – one can clearly do that sort of thing through personal offices or banks and get people to produce documentation – rather, it is the public acceptability of it. I live in a small village up in Shropshire and at the bottom of my little lane lives a lady in her seventies. She is very mobile, has a very active brain and is a strong libertarian. The prospect of persuading that lady that she needs one of these things is a daunting one. And I think that is the debate that we need to have. I am certain that, at some point in the future, these things will be around. It is a very sensitive area, and people will have strongly held, and strongly divergent, views.

**John Carr**
We are seeing more and more online gambling websites, which are essentially owned by UK-based companies. Now they took what I consider to be a very sensible view. They figured that if there were too many stories about kids going online to gamble they would be threatened with new legislation pretty quick to rein them in. So what did they do? They didn't wait for any government minister or anybody to tell them, but have invested a very large amount of money in establishing an online interactive age-checking system.

Both my kids and I have used the system, and it seems to work very well. Nothing will be 100 per cent perfect, but there, it seems to me, is a concrete example of how large numbers of people are very willing to go quite quickly towards something like that, because they can see a very immediate and tangible benefit – in this case, to do with the protection of children.

**ns survey**

50 per cent felt that children were at most risk of meeting strangers online, rather than on their way to school, in the playground or on family outings

**Geoffrey Llewellyn**
On the issue of public acceptability, we conducted some survey work in January in which there was a 4-1 majority in favour. So it certainly isn't the case that there is a huge mountain to climb in terms of public acceptance of the principle.

**Andrew Pinder**
I am not suggesting that. I absolutely accept that probably the majority of people in the country would be in favour of some sort of national identity card, and we may well come round to that. The issue is that there is a lot of work to be done to get public acceptability and build the safeguards for people who will have legitimate worries about this stuff. And therefore the arguments need to be really well rehearsed.

The key to making an ID card – a strong authentication – does lie through biometrics

There are national security and anti-crime arguments, and also some convenience arguments in relation to e-government and other transactions. So I think there are lots of reasons why one would want to introduce some sort of card, but there will be some very strongly held views, albeit among a minority of the population, and introducing these things will require enormous sensitivity.

**Scott Law**
I am sure it won't be long before we read a story about

**ns survey**

The majority felt the greatest threat to children on the internet was adults posing as children in chatrooms; a quarter felt that pornographic material was also a threat

a new electronic driving licence or a new electronic passport, and we are already talking about identity cards. One of the fears I have, when I hear talk about things like identity cards, is that there goes another £300m on some big IT project that will turn into a white elephant.

That is my fear as a consumer and I think a lot of taxpayers have the same fear that these things are somewhat ill-considered and that there are other vehicles that can be used.

**Stefan Haselwimmer**
With regard to Andrew's point about the public acceptability of entitlement cards, surely the way to enhance that is to offer decent e-government transactional services in the first place, so that people can actually see the potential benefits of having one single point of access to these kinds of transactional facilities.

**Andrew Pinder**
A cheap but effective point. I accept that.

**Simon Moores**
Recently on the BBC, the deputy editor of the *Voice* was saying that identity cards will be used as a means of discriminating against ethnic minorities. That is something I hadn't thought of before, but it is obviously causing concern in certain areas.

**Andrew Pinder**
I think there is an issue in terms of people feeling worried about how big brother might use the data. But I think there is sufficient trust in government, if the right arguments were made and the right safeguards were put in place, for things to work. But it is a very, very sensitive and very difficult area, and I personally would not want to be running this project.

**John Carr**
That brings us to the end of our discussion. We haven't reached any definitive conclusions, but at least we have illuminated some of the arguments.

# It's a bug's life

Computer viruses are bad for business. So should the government be doing more, asks **SIMON MOORES**

August 2003 may be remembered by businesses both for the record-breaking temperatures that made working difficult and an unprecedented series of computer virus attacks that, for many companies, made work impossible. In the middle of the heatwave, a wave of cyber-vandalism represented by three small pieces of computer code nearly brought the internet to its knees.

With names like evil cartoon characters, Blaster, Nachi and Sobig-F left a trail of destruction around the world. Among the high-profile victims were Sky News and Air Canada, which was forced to shut down its electronic ticketing systems. At one point, PC World reported a 163 per cent rise in the number of calls to its PC service support lines and some outlets were repairing up to 200 computers a day in an effort to clear the backlog of infected machines. In less than two weeks, and before the counting had finished, PA Consulting estimated the cost of business interruption at £500m.

The scale of the problem facing society by an increasingly lawless internet is staggering. The leading internet security company Symantec tracks more than 6,000 vulnerabilities on more than 11,000 versions of 2,700 software products from 1,300 vendors. This summer, it told the parliamentary EURIM-IPPR e-crime study group, those same vulnerabilities were turned by hackers into one million malicious code submissions, and Symantec's monitoring of the networks of 20,000 partners in 185 countries has produced data on three billion separate security incidents.

If the government's ambition for Britain to become one of the leading "information economies" of the 21st century is to be realised, then it must first solve the problem of computer viruses. According to the National Criminal Intelligence Service: "While the UK has some of the highest levels of internet e-commerce activity in Europe, the fear of hi-tech crime and the cost, in terms of time and money, of security measures may be discouraging the further spread of e-commerce in the UK among smaller businesses."

Earlier this year, a survey commissioned by the National Hi-Tech Crime Unit and conducted by NOP revealed that security incidents had cost UK business an estimated £143m over the previous 12 months. And the Department of Trade and Industry's Information Security Breaches Survey 2002 indicated that nearly half of all UK companies have suffered malicious information security incidents. However, most of these relate to virus infection and website hacking attempts. Relatively few incidents to date have involved electronic theft or fraud, with surveys showing only 6 per cent of UK businesses affected so far.

> In 12 months, security incidents have cost UK businesses an estimated £143m

The management of e-crime in the UK was a theme of the recent *New Statesman* round table on internet security, and the government has subsequently announced that it will publish a long-awaited e-crime strategy in the spring of 2004. During the round table, the government's e-envoy, Andrew Pinder, remarked that there was a pressing need for "data protection legislation to be updated for the 21st century". Since then, EURIM has suggested that the outdated and technology-neutral Computer Misuse Act, designed for a world without the internet, may soon be changed to include denial of service attacks and unauthorised access, which are contributing to a new crime wave (the subject of next February's eCrime Congress in London).

The government has played an active role in encouraging the public to embrace the idea of "Broadband Britain", and at last November's e-summit, the minister Douglas Alexander described "universal access as crucially important to the take-up of public services". With two million broadband users and approximately half the UK population now online, the government has had some success. However, there has been a cost in terms of security, and where the responsibility for this lies was a subject of vigorous debate at the *NS* round table. The government's position on the internet appears to be that it acts as both facilitator and legislator, and that security is a matter of choice for the individual and the service provider – thus legislation acts as a sanction and not a solution to a problem that increasingly lies outside government control. Some argue, however, that the government has been slow to react on matters of internet security, having been prepared to ignore security concerns in the race to deliver "Broadband Britain".

What is certain is that the kind of criminal activity that created Blaster and Sobig is now increasingly targeted at the expanding broadband network, replicating rapidly and potentially creating an army of clone computers capable of strangling the internet we so rely on, and small businesses and home users are among the most vulnerable to attacks. The question is whether the government can find a comfortable balance between progress and security. Should it be doing more, or is the widespread business interruption and computer chaos of last month simply a fact of 21st-century life?

*Simon Moores is managing director of Zentelligence (Research) Ltd*

# Working with Government and citizens towards an e-enabled society

As government and public sector organisations increasingly deploy electronic methods to increase citizen choice and service take-up, smart card based solutions will play a crucial role.

More than 20 years ago Schlumberger effectively created a new industry with the first smart card patent. We are now one of the world's leading providers and integrators of smart card solutions to the public and private sectors worldwide. At the heart of these solutions are convenience, security and privacy.

The combination of our smart card expertise with our skills in consulting, systems integration, network and infrastructure services makes Schlumberger the partner of choice for an e-enabled society.

For further information please contact Geoff Llewellyn,

agllewellyn@slb.com

+ 44 (0) 207 830 4444

**www.slb.com/publicsector**

Schlumberger