



Eversheds Lecture – Show and Tell: Is market competitiveness hindered by data protection activism and whistleblowing compensation seekers?

Speakers: **Richard Thomas**
Information Commissioner

Guy Dehn
Director, Public Concern at Work

Chaired by: **Roger Steel**
Partner, Eversheds

Date: 8th June 2004

Venue: RSA, 8 John Adam Street, London, WC2N 6EZ

NB

This is an **unedited** transcript of the event. Whilst every effort is made to ensure accuracy there may be phonetic or other errors depending on inevitable variations in recording quality. Please do contact us to point out any errors, which we will endeavour to correct.

To reproduce any part of this transcript in any form please contact RSA Lectures Office at lectures@rsa.org.uk or +44(0)20 7451 6868

The views expressed are not necessarily those of the RSA or its Trustees.

www.theRSA.org

Roger Steel: Welcome ladies and gentlemen to the Eversheds annual lecture.

A little bit about myself first, my name is Roger Steel as you've heard. I'm the head of the department for London the South and East of what we call our HRG, which is the human resources group, and in simple terms, that makes me an employment lawyer.

Eversheds, for those of you who don't know, is one of the largest law firms, and the successful law firms in the world. We have over 2,000 legal and business advisors in the firm, which is sometimes pretty daunting, but it does make a business engaged in enterprise just as many of you are as well.

We're obviously delighted in this 250th anniversary year to be associated with the RSA and to be presenting tonight a presentation entirely in keeping, I think, with the founding principles of the Society going back to William Shipley in 1754.

The title as you have heard from Liz, is 'Show and Tell: Is market competitiveness hindered by data protection activism and whistleblowing compensation seekers?' I apologise for that mouthful of what may or may not be gobbledegook. I am the author of that and I would like in a moment to say a bit about what I think it means, and why I chose it.

I think it fits in with the principles of William Shipley and the Society, in that in any free market engaged in enterprise, there has to be another side, a counterbalancing factor, if you like. What is called in Euro jargon, 'the social dimension', and I think that both the founding principles behind data protection and whistleblowing are aimed at being a part of that social dimension.

Data protection is actually aimed at supporting rights to privacy, and therefore privacy in a way is a constraint upon the free market.

Whistleblowing, on the other hand, is aimed, if you like, at attacking privacy, the privacy of corporate entities to do exactly what they like, in that its function is to protect those who blow the whistle on corporate wrong doing.

I think nobody would argue that citizen's privacy, in many circumstances, is a very good thing. Exposing fraud, equally, is a very good thing, but the issue, which we will be exploring tonight, is where does the balance lie between these good things and the desirability of encouraging enterprise in a free market economy, particularly where, I think, that economy has moved away from an industrial society to an information society.

Firstly, then whistleblowing, just a few words about what it's about, for those of you who are not familiar, its aim is to protect those who suffer detriment, having made what we call in the legal jargon, 'a protected disclosure'. Now you have to make that disclosure in a manner laid down by statute, but the sort of things which are covered by protective disclosures are crimes, miscarriages of justice, the failure on the part of the employer to meet its legal obligations, risks to health and safety, damage to the environment or the covering up of any of the above, and the legislation is called, The Public Interest Disclosure Act. It was introduced in mid 1999.

The disclosure has to be made to the employer, or in certain circumstances, to third parties such as regulators like the Health and Safety Executive or the Financial Services Authority.

A whistleblower doesn't have to be right when he makes a protected disclosure, he simply has to believe that he is right, and that belief has to be based upon legal grounds. And the legislation, as I was discussing with our speaker on the subject tonight a few moments ago, doesn't actually require anybody to do anything, it is therefore relatively simple to operate, and relatively simple to understand. It simply provides protection for those who, as they say, blow the whistle.

So obviously that sounds rather useful and entirely laudable, because I think we would all agree that if we are to engage in a free competitive market, then it is right that we be seen to be fighting fairly, particularly if we are demonstrating and holding ourselves

up as exemplars to those in the developing world.

And the other regime is data protection, a concept born, probably, 35 years ago now, when a report was issued in the growing computer age about the need for privacy, particularly in relation to electronic communications. It is obviously right in our society that things are kept private, where the information stored or obtained by somebody else is sensitive about our, for example, our health. It's right that that information should be accurate, should be kept for the purposes for which people think it is going to be kept, and that the information should not grow stale. Equally that we should know what that information is, and that there should be regulation on its commercial exploitation.

So we've had legislation since 1984, then there was the EU directive, and latterly a further UK statute in 1998, and the purpose of the law is to regulate the activities of organisations who, to use the jargon, process data about individuals who are called data subjects. A major feature of the legislation, and I suspect we'll be touching upon that in greater detail, is the right of the data subject, i.e. the citizen to access the information that is held by the data controller. Equally, an important feature of the legislation, are the prohibitions on transferring personal information outside the EU.

Now in terms of impact on business and enterprise, our theme tonight, the major impact is on the handling of information about employees and about customers, and it's a question really of, is the balance right in terms of the burdens on business in managing those processes, and are the rights given to the individual being used in the way in which Parliament intended.

Equally, a very important piece of legislation comes into force next year, The Freedom of Information Act, which will have a major impact on public authorities, and I'm sure we'll be hearing some more about that from our speaker on this subject.

So what, if I may ask the question, what is it that has gone wrong, which leads to the

question posed in the title of tonight's talk? What is it that suggests that the balance is not quite right?

Firstly, in relation to data protection, so far as the public is concerned, I think it manifests itself in a number of ways that provide an irritant to our daily lives. Ringing up the hospital to find out how your best friend is, to be told that they can't talk to you, renewing one's daughter's car insurance that one is perhaps paying for, but you can't speak to the insurer because it's not your insurance, it's theirs. Dropping into the library because you've forgotten somebody's address to be told that you can no longer look at the electoral role, those are sort of irritants that the citizen finds.

More pointed and indeed more poignant have been the recent press coverage about the two elderly British Gas customers, who sadly died in circumstances which you maybe read about, and where it was suggested that British Gas could or should have informed local Social Services of the plight of these two individuals, but felt constrained from doing so, and more recently the tragic events in Soham with the Huntley murders.

So far as business is concerned and getting back to our subject of enterprise however, it's the administrative burdens, the guidance that has been issued by the Office of the Information Commissioner, who is the official who is charged with the oversight of this regime, these cross border difficulties that I mentioned and the abuse of the data access rights. To give you an example of the cross border difficulties, it was suggested recently that Alitalia, the Italian airline, for example, has decided not to fly anymore to New York because it might be prosecuted under Italy's data protection rules for giving the US homeland security authorities details of the names of its passengers. Certainly a constraint I think you would agree on, on enterprise in that respect.

So far as whistleblowing is concerned, the question is, is the legislation actually effective in stopping corporate wrong doing? Its called The Public Interest Disclosure Act,

but where is the public interest if most cases settle and employees are paid off, leaving the employer free to carry on doing what it was doing. In other words, is it achieving its social purpose? Is it being used as a weapon by unscrupulous employees to extract further compensation from overburdened and litigation weary employers, as sometimes is alleged to be the case?

Now I have every expectation that our speakers tonight will disagree with a lot of the points that I've just made, and therefore I would like to introduce them without further ado.

On my right, who will be going first, is Richard Thomas. Richard is the Information Commissioner, in other words the official who is charged with the oversight of the whole of the data protection and freedom of information regime. He took up his post on 30th November 2002. It's right to say that he has an independent status, reporting directly to Parliament, and is therefore not responsible to Government as such.

Richard's previous career was as Director of Public Policy at Clifford Chance, the international law firm, a Director of Consumer Affairs at the Office of Fair Trading, Head of Public Affairs as the Legal Officer at The National Consumer Council and as a solicitor with the Citizen's Advice Bureau Service, so a very varied and distinguished career in public service.

On my left, Guy Dehn, who is the Director of the charity, Public Concern at Work, and I think it's fair to say that without Guy, the charity and also Gordon Borrie, who is here tonight, and many of you will know, that piece of legislation would not be on the statute book in the form that it now is and at the time when it was passed, and I think that there is no doubt that Guy and Gordon's work with that charity and its efforts has made a major contribution towards the development of the law in this area.

They will now make their individual presentations. I then kick off with the debate, which I am sure you will want to participate in, asking some questions that get put to us as

lawyers, hopefully not too aggressively, and as I say, they are not necessarily the views of either myself or of my firm, but I think they do need to be put. The intention is then to leave plenty of time for questions from the floor, after which, at around 7:30, I would hope that you would, all of you, join us for drinks. We are not at the moment quite sure where they're going to be, they may be in the vaults, but the vaults may be a bit hot, and therefore we're going to choose the coolest room we can, but we'll tell you that at the end. Richard.

Richard Thomas: Good evening. Thank you very much Chairman for showing my personal data in that way, it was with my full consent.

Show and Tell may be about freedom of information directed at the Government, but that's not tonight's subject, I'm talking tonight about data protection.

Is market competitiveness hindered by data protection law? The DTI's competitiveness hindered by data protection law. The DTI's competitiveness strategy is cast in terms of prosperity for all, making the UK the best place in the world to work and to do business. The strategy talks in terms of driving up productivity through successful businesses, excellent science and innovation, and fair markets. I'm pleased, but not at all surprised, that I could not find any reference to data protection as a hindrance, nor indeed, as one of the many challenges which need to be addressed in pursuit of the worthy objective of improving competitiveness and prosperity.

Significantly, however, the paper does contain many references to fair markets, and also to quality of life, described in terms of a goal in itself, but also a key determinant of economic performance and an important factor in competitiveness.

Perhaps I should be disappointed, but again, not surprised, that data protection is not explicitly identified by the DTI as a factor promoting competitiveness, because tonight, for reasons I would explain, I want to make the case for data protection in terms of fair

markets and quality of life, identified as important drivers of competitiveness. In other words, if we want to take competitiveness seriously, we must take data protection seriously. To put it the other way around, without data protection, markets would be less fair and quality of life would be lower.

But first I need to address and dispel some data protection myths. You will all have read in your newspapers about the Data Protection Act, this nightmare of red tape that endangers public safety, prevents effective policing, stops medical research and apparently is responsible for most social ills. We are told that data protection stops you from videoing your child's nativity play, no. It means colleges will have to ban students from using mobile phones which take pictures, no. Stops businesses sending any details of customers outside the UK, no. Prevents schools from contacting parents when there's an outbreak of head lice, no. Means you can't voice concerns about a child's welfare to Social Services, no. Stops patient health records from being used for medical research, no, no, no, no, no. The Act does none of these things.

Nor is the Act responsible for far worse ills. Without pre-empting the imminent Bichard Report into the terrible events at Soham, it's useful to repeat what Counsel to the enquiry put to me in March, when I gave evidence to the enquiry. He said, and I quote, "I'm not going to ask you any questions about the deletion of the information concerning Ian Huntley by Humberside. I know that's a subject to which you devoted a considerable amount of effort and energy in your statement, but I am not going to do it for the obvious reason that Humberside Police and the Chief Constable, in particular, have accepted now that deletion had nothing at all whatever to do with data protection legislation or any advice from your office". This independent recognition was not widely reported in the media.

Likewise who saw the British Gas press release put out the day before Christmas Eve, which effectively accepted that data protection had nothing to do with the deaths of the two pensioners whose gas had been cut off. Data protection does not prevent a gas company

from telling Social Services about obviously vulnerable customers, whose supply has been cut off.

The myths of data protection and the ease with which it can be used as an excuse or as a smoke screen cannot be ignored, and I will conclude this evening with some remarks about how we are restoring its reputation, and making it easier for organisations to get it right.

But I want to start with the impact of data protection on competitiveness. Far from hindrance, my case is that data protection is necessary to achieve a level playing field in a high tech globalised economy, where unimaginable amounts of personal information can and do flow around the world at the touch of a button.

Protecting data is necessary for businesses to thrive. Personal information which is held by a company, whether on its customers, on its staff, its suppliers or other individuals, this information is a corporate asset, which needs to be safeguarded in the same way as other valuable but more tangible assets.

Those who don't adopt high information handling standards, which is basically what data protection is all about, will suffer damage. Damage to corporate reputation, and will suffer in both customer and labour markets. To a very large extent, data protection is all about enlightened self interest. Which business wants to hold inaccurate or out of date information about their customers or their prospects? Which Bank or other financial services company, would welcome the allegation that they are cavalier with the confidentiality of their customers' affairs? Which employer wants the reputation for spying on its staff? Which non executive director is going to happy with sloppy arrangements to keep information secure? Who wants to defend their reputation as a company which gets its business through intrusive marketing methods?

Make no mistake, customers and staff care about their privacy, and they care about what is done with their information. Our

research indicates widespread prevalent and increasing concerns about intrusion and about abuse.

Half the population strongly believe that individuals have lost control over the way in which their information is used. A third do not believe the existing laws provide sufficient protection. Over 80% say they would stop doing business with an organisation, which handles information unfairly.

But the fair market's case for data protection is about far more than prospering in your domestic market. The free flow of information and ideas has long been seen as an economic driver. The OECD's 1980's guidelines on the protection of privacy and transporter flows of personal data were explicitly prepared for the purpose of promoting an international level playing field.

These guidelines were driven by a trade agenda, not just to safeguard the interests of individuals. The same is true of its descendant, The European Union Data Protection Directive of 1995, and our own 1998 Act, which flows directly from that.

The preparatory papers for the European Directive make it very clear that this Directive was seen as part of a necessary infrastructure for the information society. Data protection now is the responsibility of the Internal Market, part of the European Commission. The preparatory papers say, for example, "If each Member State had its own set of rules on data protection, cross border provision of services notably over the information super highways would be virtually impossible, and this extremely valuable new market opportunity would be lost.

Until now, differences between national data protection laws have resulted in obstacles to transfers of personal data between Member States, such obstacles to data transfers could seriously impede the future growth of information society services. The Directive seeks to promote broadly the same standards for handling personal information across a marketplace of over 400 million consumers.

Without such a framework, there will be severe difficulties with cross border trade in a very wide range of goods and services, and it is not confined to European trade, driven in part by provisions in the Directive, which restrict the export of personal information unless there are adequate safeguards. Most developed countries now have or are developing a privacy or data protection regime, which bears close resemblance to the European model."

Let me divert a little deeper into history, both to place data protection into its fair markets context, but also to pave the way for what I want to say about quality of life.

The first modern data protection law was adopted in the German land of Hesse in 1970. The Germans, unsurprisingly, retain a reputation for being very keen on data protection, as do many Europeans who have suffered oppression.

During the Second World War, and for nearly 50 years afterwards, various regimes across continental Europe has special parts of their security operators specifically tasked with examining records to find useful information, such as that concerning ethnicity or political opinions of those living under the occupation. Apparently magazine subscription lists were of particular interest to these people.

Data protection law grew very much from a post war fear of secretive, excessive and intrusive information gathering by state institutions. It was thought that the coming of computers would accentuate the problem, giving the Secret Police and state surveillance agencies greater power than ever to gather and analyse information about people.

It's not Orwellian scaremongering to recognise that totalitarianism plus massive surveillance power amount to a frightening combination. And it's difficult to talk about the origins of data protection as a defence against totalitarianism without seeming evangelical or ignorant of the difference between democratic societies and non democratic ones. However, I think that understanding of the historical origins of data

protection is necessary to understanding its current purpose. It explains the heavy cultural weight attached to data protection, very much as part of the human rights agenda, fundamental rights and freedoms across continental Europe. Its why, if we want trade to flourish, we need to take data protection seriously as a fair markets issue.

But this historical perspective also has a bearing on the quality of life arguments. Quality of life has many attributes, but these must include our relationship with the state, our place in society, our self worth as individuals, and our personal privacy and autonomy. The quality of life arguments for data protection reflect its safeguards for all of us as individuals against the actions or misdeeds of powerful organisations. It is about human rights and human values. It affects all of us. It's relevant to all of us because we are all subjects of the increasing amounts of information the society generates, records and analyse.

We now expect to be told routinely, how our personal details are going to be used, that we can stop unwanted junk mail and that credit will not be refused because of the bad payment record of those who lived previously at the same address, all data protection achievements.

Many have used the Act to gain access to their own files. Some have needed to take action about inaccurate information causing real damage to their lives. That is making requests for access to records, for example, to Government departments or financial institutions, are often surprised by the scale and complexity of the records that exist. We get about 12,000 complaints a year about the keeping of personal records, inaccurate health records, mixed up police files, confused credit reference information, excessive information, improper disclosure, failure to disclose and so on. We daily see the sorts of problems people can experience in the information society, often raising matters of real substance, cases where individuals have suffered real detriment from poor information handling practices.

I think of the copy of the Children at Risk Register found on a second hand

computer, of the cameras hidden in a fire alarm in a hotel bedroom to spy on the guests. I think of the man repeatedly refused employment because a record of a minor misdemeanour in his youth had been improperly retained on his police record.

Not everything that happens in the information society is benign. There are risks for individuals when too much information is collected about too many of us, or when significant decisions are based on inaccurate information. The individual needs a defence, a set of standards which they can rely upon, a chance to say no to the over inquisitive official, a right to demand that inaccurate records be corrected.

Without data protection there would be no limits or restrictions. Organisations would be free to collect as much personal information as they want, to do with what they want, to pass it on to anyone else and not to worry about mistakes or security lapses, and to keep it as long as they want. Not a comfortable or happy state of affairs, not great quality of life, even in a fully democratic society.

And these issues are especially important when the actual or potential detriment can flow, in those situations where competitive pressures are lightest or non existent. That's why I attach particular importance to data protection safeguards, which protect the individual against the state, and indeed against the whole of the public sector, which is not faced by a competitive market place, and the pressures which I outlined earlier. If the state gets it wrong, there can be serious consequences for tangibles, our liberty, our health, our ability to earn a living as well as to the less tangible aspects of privacy.

The issues are especially acute with law enforcement and areas such as child protection. Too often there are perceptions, wrong but real, that data protection stops people doing sensible things. Two contrasting examples show how hard it is to strike the right balance when it comes to information sharing.

In 1999 Patricia Goddard was murdered by her husband. In the previous five months, six different agencies, health, police, housing and so on were aware of her problems and the abuse she was suffering. None had informed anyone else about their concerns.

A year earlier, 1998, another lady, Gina McCarthy had also been killed by her husband. In this case the courts had ordered her to send a monthly progress report via Social Services to her husband. This had passed on her secret address to her husband, he had found this, he had murdered her as a result of that information, improper, wholly unacceptable information disclosure.

Of course we want our health and social workers to safeguard vulnerable adults and stop children being abused. We want the police and other Government agencies to protect us against crime and terrorism, but as a quality of life issue, no one will suggest that such agencies should have unlimited powers to do whatever they like with our personal information or our privacy. No one wants them without any controls at all, to build vast databases on every individual, to intercept our phone calls or snoop on the content of our emails.

Equally, of course, we don't expect the police, the security services or social services to ignore personal information when dealing with real cases and real risks, or indeed tell us everything they're up to. That's why there are Data Protection Act exemptions covering these areas. But these are exemptions. The general rule is that fair information handling practices should be adhered to.

But there are risks if we go too far. A combination of pervasive CCTV, facial recognition technology, databases of biometric features, vehicle tracking cameras and the massive trail of telecommunications data we all leave in our wake could lead to a society where we're continually being watched, and our actions recorded where the innocent have no right to a private life to enjoy.

Its interesting when reading accounts of those who've lived in a fully fledged surveillance society, there's not just the political crimes, the arbitrary arrest, the human

rights abuses that made life so dreadful. It was the feeling of being watched, the knowledge that dossiers of thoughts and actions were being compiled.

So I need to ask how the development of a surveillance society could affect us, whether it will stunt our development as humans. The current debate over identity cards, a matter of major significance to my office, has brought many of these issues into sharp relief.

This afternoon I've been giving evidence to the Home Affairs Committee about the draft identity card bill, which is really in fact all about setting up a powerful, national identity register, and I think there's a lot of debate to be had on that particular issue.

It's quite easy to put a price on crime, to add up stolen property and the fraudulently claimed benefits. We can establish the cost of damage to health or loss of life. The value of privacy though is more difficult to calculate. What units do we use to calculate it? How much loss of privacy is justified by a 10% reduction in crime?

Valuing access can be equally difficult. How do we weigh the value of a person securing access to his or her records against the expense to the organisation in granting the access? Of course it depends on the circumstances. It's clearly of enormous importance to the individual, who finds that the incorrect or grossly out of date police record has been blighting their career progress.

It's of similar importance to the employee to gain access to their personal record, which then reveals they were passed over for promotion due to an inaccuracy or to a prejudice, and these are exactly the sorts of circumstances where people seek access to their records, because they want to check that they are being treated fairly.

I talked to you earlier about the myths of data protection. Why then is there so much misunderstanding, and so much misconception? The values of data protection are attractive; they make sense both for those

who keep records and those about whom the records are kept. The backbone of the, so called, data protection principles, there are eight of these; they are simple, attractive, uncontroversial. They require personal information to be obtained and handled fairly and lawfully. To be obtained for specified and lawful purposes. To be adequate, relevant and not excessive, to be accurate and up to date, not kept longer than necessary, processed in accordance with individual's rights, kept secure and not transferred overseas unless there is adequate protection elsewhere. In addition, certain key rights including access to information to prevent records being used for direct marketing, to obtain compensation in certain circumstances, and to have records rectified, blocked or erased in certain circumstances.

I don't think there's anything controversial here. I'm sure these are all standards we'd all wish to buy into and rights which we all feel should be available to us. These are the standards which ordinary people rely on as a defence against some of the deficiencies and excesses of our information society. Which of these principles or rights would you be happy to lose for your personal information?

The problem, which I believe is largely responsible for the myths and for the poor reputation, is that both the Directive and the Act are not at all well drafted, in fact they are and they are widely seen, as opaque, complex and scary. The language doesn't help. Who, outside the very tiny data protection community, talks of people as data subjects? Why does the law talk of personal data, rather than simply personal information? Who is really comfortable with a schedule 2 condition for processing? Do you know that you are the subject of an accessible record held by your health professional, or that if you are engaged in a processing of eligible manual data, other than that forming part of an accessible record, then you may enjoy transitional relief? Perhaps it would help a great deal if we simply gave the Act a new name. How about, the Protection of Personal Information Act?

But the problems of the law go deeper. It's an extraordinary mix of general principle and detail prescription, which makes the Consumer Credit Act look very straight forward, Gordon, within a convoluted framework. It was described last year by the Court of Appeal, as cumbersome and inelegant. Quite rightly the Act regulates the automated processing of almost all personal information, but it's less explicit about the desired results or the different degrees of detriment.

Despite these criticisms, it's simply not politically realistic, domestically or at the European level, to think in terms of any imminent wholesale changes to the Directive or the Act.

As Commissioner, I have to be realistic. I am responsible for promotion and enforcement of the law, not for its content. But there's a great deal I can and I will do to make it easier for organisations to cut through the gobbledegook of a legislation and to get it right.

Likewise I need to concentrate our efforts to make sure that individuals are safeguarded where it matters most. That's what I mean by restoring the law's reputation, and that's why our new corporate plan, which we launched just back in March, spells out the priority and I quote, "of taking a practical, down to earth approach to our data protection activities, simplifying and making it easier for the majority of organisations, who seek to handle personal information well, and tougher for the minority who do not".

And behind this our new approach anticipates many new features including, guidance in plain English with clear, concrete answers, new codes of practice, an enhanced telephone help line, new criteria for enforcement action concentration on cases of deliberate non compliance, cases of serious detriment, cases where an example needs to be set or cases where enforcement, in fact, will actually clarify ambiguous law.

And also this time last year I launched the so called, 'Make Data Protection Simpler Initiative', and we're following up various

changes of our own policies and procedures in response to what people tell us, where there's clearly scope for de-mystification and simplification.

Our new approach recognises that there have been quite a lot of confusion over the years about data protection law, and perhaps an excessively zealous or even theological approach may have been taken in some quarters. It recognises the foundation of a law, its fairness and common sense, largely reinforcing what enlightened organisations should be doing in any event.

Fundamentally, data protection law, what it does do is force organisations to stop and think. Why are we collecting this information? How are we going to use it? How much do we need? Are we keeping it accurate and secure? Have we told people what we're doing?

But perhaps over the years, some of our guidance, whilst essentially right and legally accurate and legal in policy terms, has been too long, has been too convoluted and has been too confusing for many people. We've relied far too much on the terminology of the law itself, and one example, which may perhaps feature in discussion, is our new employment practices code, where we took a much more deliberate attempt to write this in the language of employment human resources specialists, in large, medium and very much in small businesses as well.

So my time is up. I will conclude at that point. I've tried to keep within the time. I think I'm just about doing alright. So my conclusion is that data protection law does not hinder competitiveness. It does require organisations, public and private, to take an approach which they can justify, but leaves them with far more freedom, far more flexibility than many appreciate. And this, domestically and internationally, is entirely consistent with the need for fair markets, and is entirely consistent with improving quality of life for individuals.

How can we be competitive if organisations hold inaccurate information, have poor security or have lost the trust of the public? And the first to concede that the law

can at first appear to be complex and burdensome.

This has contributed to negative perceptions and suggestions of excessive burdens. That's why my office needs to communicate clear messages about the practical, down to earth, common sense approach. We will seek to keep the regulatory burden to a minimum. The law may appear to be scary sometimes, but the world would be a great deal scarier without data protection. Thank you very much.

Guy Dehn: Thank you very much Roger. Can I also thank the RSA and Eversheds as well for inviting me, and thank you for coming?

I apologise that I haven't written a paper but the reason is that what I want to say is a bit of a work - or thought - in progress. So please feel free to correct me or disagree with what I have to say.

It's an honour to follow or succeed Richard Thomas, though not for the first time as about 18 years ago, when he left the National Consumer Council in 1986 I succeeded him in one of his roles there as Legal Officer. And that's where I want to start considering the issues raised by the question: "Show and Tell: Is market competitiveness hindered by whistleblowing compensation seekers?" In this brief talk I want to look at rights, remedies and redress; I want to look at market competitiveness; I want to look at the way that the whistleblowing legislation was structured, what we were trying to do and whether and how we see it now working.

So when I succeeded Richard in 1986, the consumer field in the UK - with an enormous contribution from Gordon Borrie and others - had seen a huge shift toward a rights-based culture during the 60s and 70s. One driving force behind this was the inequality in bargaining power between the consumer and the producer - and this was caused in part by contracts set by the producer. To address this, a lot of legislation was introduced on sale of goods, on product safety, on trade descriptions and whatever, which was trying to give equality of arms to

the consumer. Indeed outside of the consumer field, similar shifts were happening in housing and other areas.

Around the time that I took over from Richard, there was a slight shift, and that shift was away from rights, because we'd had 15 to 20 years of legislative rights, and the debate was starting to look at redress. People were saying, "There are all of these rights, but what do they mean, what use are they, how can I get to enforce them?" Campaigners and lawyers were saying, "People need to have access to justice". While I'm a devotee of the idea of access to justice, I'm not quite sure that when I think of access to justice, I'm thinking of the same thing that lawyers or other campaigners are thinking of.

Whether or not this was due to the way the legal aid system funded cases and the change in nature of legal advice and services that that spawned or coincided with, it seemed to me that the phrase 'access to justice' was being used as a synonym for 'access to litigation'. It was about redress, about being able to get into court. But from my experience as a barrister and in free legal advice centres, it seemed to me that, for the individual - whether it is an individual consumer, employee or citizen - litigation is a mostly miserable experience.

I suspected that a fair many cases that were litigated were ones which the lawyers themselves might have been slow to litigate had they been the client. It may be they had advised their client of the downsides and risks and the client had made an informed choice, in which case I have no issue at all. But speaking personally, I would need to have suffered something quite substantial to go into litigation, and the reasons for this are its time-consuming, it's costly and what you're doing is reliving the bad experience. And it's also worth noting, when one talks of moves to secure an equality of arms in terms of rights, that when one comes to litigation - and this is the way it is and I'm not saying there's a better way than the way that our system operates - there is not what the public would see as an equality of competence of the lawyers that are needed to litigate on equal terms. You've got the legal team you've

got, and if your opponent has a much better lawyer, they are going to have a much better advantage than you when any redress is to be decided.

It may help illustrate this point about access to justice and litigation if I use an analogy that we use at Public Concern at Work when we advise prospective whistleblowers or those who may have a claim, or may be in an early stage of one. This analogy is drawn from the health service and going to see your GP.

If you've got a pain in your heart, or a pain in some part of your body, and you go to the GP, he'll ask you what's going on and why, and then he may say, "Take some more exercise" or "Have you thought of taking half an Aspirin a day" or "Cut down on your fatty foods" or some such. But if most times people went to their GP with such a pain, the default response was that you need open heart surgery, people would start to think that's a bit over the top.

So in the same way I think assuming that access to justice means access to redress is mistaken. For individuals I equate litigation with open heart surgery - it's very necessary as a last resort. I simply don't think very many individual litigants enjoy litigation or would recommend it to friends. I accept there are some who want to have their day in court, but for your average Joe or Jane, I think litigation should be viewed as an unhappy experience. This is particular the case where the litigation arises out of an on-going relationship - say in the family or in one's work - because such relationships cannot reasonably or realistically be expected to survive litigation.

One other point about a redress mechanism is that it is the means to award compensation - that's what I imagine probably 99% of all litigation in this country is about. There's an award of compensation at the end of it; monetary compensation for losses you have suffered, so of necessity it's mostly backward looking and when it looks forward it only considers a dismal and distressing future.

Now this is one of the reasons that I think law is a blunt instrument and here I want to pick up a point that Richard was saying about the myths on the Data Protection Act. Shortly after the whistleblowing legislation was passed, we did quite a lot of open training, some with law firms, which was given back to back with data protection training. What became apparent to me when I sat through one of the half-day Data Protection Act training sessions for HR, information and in-house legal people was that the abiding message they were all left with was, do anything under this Act without taking legal advice, and you're probably in real trouble.

Now I don't know whether there was someone from Humberside Constabulary there at one of these sessions, but if there was then that may be one of the explanations for what happened in Soham. While I don't know whether it's within the vires of the Information Commissioner, I would personally far rather that when people have a data protection problem that they would consider going to the relevant regulator and saying, "What about this?" rather than going by default to their lawyer.

Now I am a lawyer myself, a poor lawyer, and I want to make clear I have great respect for colleagues and for the many brilliant lawyers around – many of whom have provided invaluable advice and help to us at Public Concern at Work. But what some lawyers do, being highly intelligent, very gifted people trained to focus on the argument, is to test the law, and for some it seems that the most enjoyable thing they can do is test a law to see not just whether it's a blunt instrument, but whether they can make it into a pointless knife.

I now want to look at competitive markets, and there's an important contrast here from the way the legal system operates and one which I think I and colleagues in the consumer field did not fully grasp. There we had focussed on the importance of rights and then - in the last 15 to 20 years - the emphasis has been on redress or access to justice.

In my view competitive markets have a number of great virtues, one of which is that

they are brilliant on remedies. So we have the three Rs - rights, remedies and redress - and what competitive markets do, and the reason they are so good on remedies, is that they look forward because they are based on the producer's fear that it will lose custom. Its not just that that particular transaction didn't work that matters, what the shop or producer in the competitive market is worried about is if he doesn't do right by that customer, he or she will go away and not come back, and the chances are that customer will tell other people and they won't come back.

It's a completely different psychological structure that we're looking at between access to justice and competitive markets and in a real sense a truly competitive market is one where the self-interest of the producer is very closely aligned with the interest of the consumer, namely to satisfy the consumer, and that is a major driving force.

As an example, if you've got two greengrocers down your street and you go into one and you buy some onions, and the onions are rotten, and you go back, if you think it's worth it, to that guy and you say, "Those onions you sold me last week, they're rotten", I bet you he's not going to say, "Sod off", he'll say, "Have a couple of bags. Oh, I'm ever so sorry". So the remedy for him, in that situation, what he is giving you, is double the amount of onions of the original transaction.

I think that when you're looking at competitive markets it's worth remembering this. Where you've got markets which aren't fully competitive in that way, I think one of the driving forces - and either Gordon Borrie or Richard, as both know much more about these things than me, can correct me if I've got it wrong - is the fear of failure. And the fear of failure can work in a fairly effective market where I believe 20-25% of customers are able to move without much hassle. This is because if they're able to move, then you want to make sure they have no reason to move; you want to keep them sweet.

So looking at it this way, a competitive market encourages its actors to be

forward looking. Because the remedies that are available to the customer are linked to the sanctions on the supplier and really quite substantial, the means of redress – or dispute resolution - isn't built in as the first option. This is not to say that markets in the UK are all fabulous and that there aren't real problems, but to me, if a market is truly competitive it is great on remedies and that has a real public interest benefits in itself because it focuses first on prevention not cure.

So, to recap, before I turn to whistleblowing, where my mind is, is that we've had a situation where there's been a lot of focus by politicians, lawyers, consumer activists and public servants on rights and redress, and we haven't looked enough at the issue of remedies. I think that when we're developing a law, we should much better consider these three Rs together and so see if we can harness some of the benefits of the legal approach and the market approach. If we succeed then we'll probably end up with better laws and, I think, with a better system.

And having said that - I'm going to expose myself to ridicule – that was actually one of the things which we were trying to do when we were developing the whistleblowing Act. I don't know whether what I've said has been comprehensible or coherent, but assuming it was, I should add that our thought process at the time wasn't as considered as I'm trying to justify now.

The whistleblowing legislation was based on a mutual self-interest between organisations and the people who worked there and the public interest. In constructing it we looked in the round at the sanctions and the remedies, and not just at the issue of the financial compensation for a whistleblower who was victimised. It was about how the law operated but also about the dynamics around it. Because you don't just have the law: you also have the media; you have the effect on fellow workers, on shareholders and others. There are lots of different factors to consider. If you put blinkers on and you think law, rights, redress, been there, done that, yeah sure, you're talking about bureaucracy and prescriptive regulations. But if you can see how the issue operates in the

round, about the different factors which affect the tension between the law and its practice, then I think you ought to be able to get something which is a bit more workable.

The main aim of the whistleblowing legislation was to deter wrongdoing, and as Roger has said, there's no problem with that, everybody will salute that flag. The way that the legislation sought to do that was by preventing the victimisation of a genuine whistleblower. I think I'd like to point out an additional difference between the Public Interest Disclosure Act and, as Richard set out, the background to the Data Protection Act with the Council of Europe Treaty, then the European Commission Directive, and then with the UK's own Act and how that was all put together.

The whistleblowing legislation was started in and by Parliament, with the call coming from backbench MPs. When it was considered, it was always considered under what's called a private member's procedure, so there were no whips, just free votes. So all you needed was one MP to say 'no' or essentially to carry on talking, and the legislation would fail.

Now when you've got that sort of situation, you've got to get your ducks in a row, and that was a great incentive to us. It wasn't a bind and I don't regret it for a moment - it meant that - apart from drawing on the practical experience we had had at Public Concern at Work - we and our colleagues at the Campaign for Freedom of Information went and we talked to business, unions, regulators, individual companies and professional bodies about how it would work in practice and what their concerns were. We had a better understanding of what their concerns were and how one might deal with them, and there was much a better buy in from them. And in that we were greatly helped by the Bill's promoters in Parliament: Tony Wright, Don Touhig, Richard Shepherd and Gordon Borrie.

Now I'm not saying it's a trouble-free piece of legislation, but certainly it doesn't have the adverse press that the Data

Protection Act has. There is no bureaucracy in the Public Interest Disclosure Act (PIDA). So as to the question I was asked at the beginning - is the idea of a vibrant, competitive UK put at risk through the introduction of bureaucratic regulations like PIDA? – the self-evident answer is no, not when you come to whistleblowing, as there is no bureaucratic regulation in it at all. The only thing the legislation says is, if you victimise a whistleblower wrongly, you will be expected to compensate them for their losses. End of story. There's no requirement on any employer anywhere in Britain to do a single thing under this legislation. So as to bureaucracy, it's just not there in the whistleblowing law.

In fact one of the drivers behind PIDA was actually to try and check the growth of the knee-jerk bureaucratic response that would hinder market competitiveness and would damage public confidence in public life. This had so often resulted from the many disasters and scandals of the 80s and early 90s such as the Zeebrugge ferry disaster, Piper Alpha, Clapham Rail and Robert Maxwell. These gave real momentum for a new approach to whistleblowing as time and again it turned out that staff were well aware of the dangers and had either said nothing or raised the concern in the wrong way or with the wrong person.

Take Robert Maxwell. Our Scottish director is a man called Harry Templeton. He used to work for Maxwell; he was a shop steward and a printer at The Daily Record, the Scottish equivalent of The Daily Mirror. He tried to blow the whistle on Maxwell to no avail, challenging Maxwell and his abuse of the pension fund, trying to get help from the unions and professionals, trying to raise the concern internally. For this he was sacked and at that stage he was about 42, he had five kids, I think, he was the only bread winner in the family, he had spent all his life as a printer, and he was sacked and Maxwell said, "And you're never going to work in the industry again". Maxwell was able to deliver on that. The guy was paid off with £25,000; the maximum amount of compensation at that time was £12,500.

What was the response when it was proved that Harry was right, a couple of years

later, when Maxwell died and they found out the pension fund had gone? The response was a bureaucratic bean feast. I don't want to sort of criticise anyone, but actually the regulatory regime that was set up on occupational pensions as a result actually meant thousands of British companies closed down their occupational schemes. This was before the financial problems came. It just became too bureaucratic to keep those schemes. So when we're looking at market competitiveness, remember: whistleblowing is a means to promote, entrench and advance market competitiveness, so no sane person should buy this argument that whistleblowing hinders it.

So to see how the Act is actually working, let's look at some evidence. There are each year close to 100,000 employment tribunal claims. Each year since whistleblowing legislation has been in force, there have been less than 750 PIDA claims. Does that sound like abuse or overkill - less than 1%?

Remember also that if you're a white male in your first 12 months at work, the only legislative protection you've got, if you're able-bodied, is under the whistleblowing Act. The whistleblowing Act is also one of the only bits of legislation which protects you against detriment, that is victimisation short of dismissal. And importantly, it's one of the only pieces of employment legislation where awards are uncapped. Now with only 750 claims a year, I have to say that the idea that it's hindering good governance or market forces is completely beyond me.

So the structure of the whistleblowing Act is to say that there should be an early and effective addressing of any significant risk. It's trying to get the employer to create a culture where an employee has the confidence to raise a concern internally and to get everyone to recognise the accountability that runs from the employee to the employer, the employer to the regulator, the regulator to the wider community. That is the approach that it's built on and is the clear message of its disclosure regime. In this it's closely linked to

the approach of a competitive market, because it has a lot of fear built into it.

You don't want to victimise a genuine whistleblower, because if you do, not only will you have to pay them compensation, but when it goes to court it will attract media publicity of the original problem you were trying to cover up or trying to deflect. If you deal with the matter properly, there's no problem. So again this is right back there with the common sense and simple approach of the market.

The legislation was designed, as I said, so there's no requirement on anybody to do anything. Its approach was as if to say if an employer wants to use this for its advantage to deliver its accountability, to make a more open workplace, a more efficient one, to explain a shared interest the employer and employee, then they can do that. That's their choice. There's nothing in the legislation requiring it, but if the employer doesn't take that opportunity, then they leave the legislation to the employee, and the employee might try and see if he can use it to his or her own advantage, and not just the public interest. This is one reason we regret the fact that the only promotion by the Department of Trade and Industry of the whistleblowing law has been as a means to sue your employer, rather than as a governance tool.

Also let's not overlook the fact that nobody begins to have a claim under the whistleblowing Act unless they have made a disclosure about wrongdoing, they have made it in good faith, they have made it in a responsible way, and they have been victimised for it. So there is no automatic 'show and tell', as the title to this lecture suggests. There will be no 'show and tell' in PIDA, unless the employer has given an employee good reason for that employee to go outside, to go public, and has then victimised him for doing that.

Now there is a problem, which Roger identified, and that is that some employees - whether with advice from unions or lawyers or not - who look at the legislation or find out about it, and they think to themselves, oh gosh, unlimited compensation, I think I might try that one. Well our point is, that any employer who

allows himself to be blackmailed by a bogus whistleblower, is making a big mistake and is being very ill-advised. One practical reason for this is that however they sort it out with that one employee, that employee is going to tell a couple of his mates when he sees them, and they'll know what happened, and it will trigger someone else to try their chance. It can only encourage employees to keep concerns of wrongdoing in their back pocket to use at some time of their choosing and at their convenience, with little regard to the public interest or the interest of the employer. I want to stress that there's a responsibility on employers to behave responsibly in looking after the public interest.

Now when the legislation was passed, the information on PIDA claims was on the public record, and this was a very significant thing. Parliament understood that and we thought it was very important. It meant that if someone at Public Concern at Work suspects that I'm stealing the charity's money and they raise this with trustees and we foolishly decide to sack them for this, on the basis that when they bring a claim we can buy them off and cover it all up, that's a non starter. That wouldn't happen under PIDA as the information of the claim would be on the public record and this meant that people would be able to see what had happened and I or my trustees would be expected to account for our actions - whether the allegation was mistaken, mischievous or well-founded.

After this right of access has been confirmed by the High Court, I am sad to report that it was reversed by secret bureaucratic regulation for reasons which, inasmuch as we could understand them, were gravely confused. I'm pleased to say that the Department of Trade and Industry have indicated to us that they are now prepared to revert to the original and correct position. In other words one where the information about PIDA claims will be on the record again.

Now once the information on the claim is open and on the public record, and from what Roger has said, I look forward to Eversheds support on this, any threat of blackmail will have disappeared or been

greatly narrowed. So if an employee comes along and says, “You know, unless you give me £100,000 I’m going to ruin you and I’m going to bring a whistleblowing claim” the employer should say, “Look, I’m ever so sorry, you bring a whistleblowing claim, that’s on the public record already, you’ve got no bargaining power over us by blackmailing us, we’re not going for that”. So that’s a very strong, positive thing, and if the basic principle of open justice is respected – as it simply has to be when Parliament has legislated on public interest disclosure – then whatever little abuse there is, I think that’s going to go away.

So let’s go back to the big disasters I mentioned. The Inquiries into those showed the need to address the breakdown in communication in workplaces and not just the systems and processes by which organisations have to operate. First, in the UK we have seen a bit less of them than in the late 80s and early 90s. There are many factors for this – consumer expectations, changes in leadership, new laws, refined regulatory approaches – but one small part may have been played by the whistleblowing law. Leaving the UK, we’ve seen Enron and World Com – where there was no legislative scheme and where whistles were not blown for years: were they good examples of market competitiveness? Is that a really great thing to fictionalise all your accounts, when the other guys who are actually trying to supply the electricity and the energy are going out of business? No, I don’t think so. So I think the people who, late in the day, blew the whistle on Enron were doing us all a good favour and I think if the US had had legislation like PIDA maybe those problems would never have got to such a disastrous stage for so many.

Not all is perfect here in the UK. Look at what’s happening in the sorry saga at Shell now. What does that tell us about market competitiveness? What about all those people who had shares in Shell or who were buying shares? “Oh my adviser says they’ve got enormous reserves of oil, that’s wonderful, that will secure a good long-term return so I’m going to stick with Shell”. But I bet you if you’ve got those shares, you would far rather that someone had said, “Hang on a second, we

haven’t got all those reserves, we’ve only got two thirds of them” or whatever the figures were. And if that had been the culture and the practice, the market would have been able to deal with it. So again, market competitiveness is seriously advanced by whistleblowing.

And I’m very pleased that what’s happening is that it’s not just us saying this. The new Combined Code, which is the corporate governance tool - not a bureaucratic regulation, not a legislative requirement but produced by leading businesses, and their advisors – puts a very sensible incentive, short of an obligation, on listed companies, to promote, review and monitor their whistleblowing scheme and practice. This will help get the message across that if an employer wants to use PIDA for their competitive advantage they can. It’s there but they will need to promote it to their staff. If they don’t promote it, and their staff don’t understand it they will confuse public interest with private interest, and then you go down the slippery slope that I suspect Roger may pick me up on shortly.

One of the important things is, as the culture changes and people who are bona fide whistleblowers are not discriminated against in their careers or job prospects, then obviously the prospect of large sums of compensation decline, because one of the important things in the law is the duty to mitigate. This means that whatever loss another has caused you to suffer, you’re not meant to just sit back and buy yourself a packet of Havana Cigars and a big bottle of bubbly and say, “I’ll never have to work again”. You have to go out and try and pick yourself up. So the duty to mitigate is very important and as the culture changes, even where the odd whistleblower is victimised, he or she should find that it is not the end of their career and if that is the case, there will be no need to pay them large compensation as if it were.

So can I conclude first by thanking you for listening to me. As to the lecture, the whistleblowing Act has had the opposite effect to that raised in the question. There is no regulation, there is no bureaucracy, there is

scant abuse and it's been and will be a positive help to market competitiveness. Thank you very much.

Roger Steel: Right ladies and gentlemen, I'm sure you will have lots of questions of your own, but if I could just ask myself, a number of questions of each of our speakers, because I feel they have been consummate politicians and defenders of their own regime tonight, and I don't think I could let them off that lightly on a number of subjects.

So first for Richard, you mentioned in relation to guidance, that it was your aim to simplify and not to confuse. I think it's the case isn't it that in relation to the guidance on dealing with employees, that whereas there was one set of guidance, we now have it in four parts, that the sum total of four parts is actually longer than the first part, and that in relation just to one of those parts, that on employee monitoring at work, that the primary guidance is 42 pages long and so is the supplementary guidance. Is that actually helpful do you think to businesses, particularly small businesses?

Richard Thomas: If I can quote somebody, no, no, no, no.

The employment code was getting a pretty bad press when I arrived. The draft on surveillance in the workplace ran to about 58 pages, and was heavily criticised for being... attempting to be 'one size fits all', and sending out some very sort of dense messages.

We pulled the plug on that and we reduced the core code to 22 pages. We also adopted, what I might call, a marketing segmentation approach, which is that 'one size does not fit all'. So we produced a small business version, which was 6 pages long, and we then recognised that some organisations, the very large multi-nationals, the government departments, others wanted more detailed insight into our thinking and so we produced supplementary guidance for, if you like, the cognoscenti, who needed to have a deeper insight. It was not part of the code, it was on our website to allow them to understand our thinking, and that's where the longer pages come from.

Financial Times aren't always our best friend. They described the new code as a model for any organisation across the world. So I yield to nobody in our defence of the new approach with the employment code.

Roger Steel: It costs only £10 for an individual to require an organisation to produce the appropriate information, and that has to be provided within 40 days of the request. I think the complaint is that that provides an uneven playing field in litigation, allowing plaintiffs access to the defendant's documents at a time before the defendant has an opportunity to see the case against him, and that actually data protection is now a weapon of choice in litigation, creating that unfair playing field. Would you agree with that?

Richard Thomas: A number of issues there. I articulated the case in favour of accessing records, and I believe that £10 is about the right sort of charge. It is not high from the point of view of the organisation, but very much higher would be a barrier for the individual. Bear in mind that it is almost exclusive, not quite, but almost exclusively now access to computerised records. It's been there for 19 years like this, hasn't caused major problems. Most organisations can deal with the requests, you know, well within a sort of threshold of £10 cost.

You raised the point about giving people, sort of, unfair access to documentation when there is, to quote Guy, 'miserable litigation' in prospect. The Court of Appeal in the Durrant case last year had some negative things to say about that practice, which I think were broadly ones which I would support. The Court of Appeal, that case last year, also largely excluded manual records from this process, and I do fully accept that it was very burdensome on organisations to go through extensive manual records for £10, but I think the new regime is a lot more sort of focused now.

Roger Steel: It's the case isn't it, that actually the more chaotic you have a filing system, the less likely you are to be caught by your legislation.

Richard Thomas: That's one way of putting it isn't it, yes, but I think I would say, the better your record keeping, you know, the easier it is to deal with requests, and I think for 19 years now, most organisations collecting personal data know that there is a, if you like, a possibility of someone looking at their records, not for litigation purposes, but for the purposes which I articulated.

Roger Steel: And you suggested that it is actually quite easy to carry out an electronic search, whereas if people have information in personal folders, which require overriding password protection, have sensibly put things on hard disc etc. to suggest that you can search through several computer systems across a very large organisation well within, as you put it, the parameters of £10. I think it's somewhat unrealistic isn't it?

Richard Thomas: I'm not saying you can do it every time, I recognise there are some problems with archive material, off site material, we have, you know, some concerns on that. The Department of Constitutional Affairs, which is the policy making part of the operation, you know, has been reviewing the arrangements and we're not unsympathetic to some fine tuning in that sort of area, but I think the general point I'd want to make, Roger, is that the vast majority of organisations don't find it unduly burdensome.

Roger Steel: And in relation to due diligence, when one company is taking over another and is looking at the financial health or otherwise of the target organisation, would you accept that the bureaucratic need to redact names of people in relation to the salaries that they earn etc. is an undue burden upon business in that particular exercise.

Richard Thomas: I think you're talking about redaction of third parties, because I do recognise where someone wants to see their own information, if the same file's got someone else's information, that's a breach of their privacy and we argue the case for redaction. Again, many organisations now make sure they separate the stuff out, so there's not a problem in the first place.

But I think I would just raise a slightly wider response to your questions, and it partly reflects Guy's story about, you know, going to the law firm and, you know, people going away very scared about the legal requirements. Don't forget that when we deal with cases, one of the tests we apply is, does this reveal a matter of substance. If there's no substance to it, we won't do anything more, so I find myself in a slightly curious position sometimes as a regulator, that many organisations seem to be sort of over regulating themselves, taking it too seriously, and...

Roger Steel: So you would deal with a light touch.

Richard Thomas: Light touch, yes, I'm not going into lawyer bashing, I will... I talked about my 'make data protection simpler project', my unkind colleagues talk about, 'make data protection pay projects', but we're not into lawyer bashing, but I think sometimes it has been taken with, I used the phrase in my speech, 'an over zealous approach in some quarters', I use those words quite carefully, and I think some people have lost sight of the fundamental sort of rationale and reason for legislation.

Roger Steel: And finally for you, Richard, you mentioned the transfer of information outside the EU, and the difficulties with that. Is it not true that the attempts to get around that problem with, what are called, the 'safe harbour principles' in the US, have had a very low take up, that the attempt for the binding corporate rules for the transfer of personal data within multi-nationals, that the EU Governments can't even agree between themselves, as to how that should happen, and that the whole issue of the transfer of personal data outside the EU has been a commercial disaster?

Richard Thomas: No I wouldn't go as far as that, but I would first certainly recognise that there are problems. We have the lightest touch in Europe. In every other European country apart from Ireland, you have to get the prior consent of the regulator to explore personal information outside the

European Union ((?)) certain safeguards. We don't have that in this country, we say, it's for you as the organisation, the data controller, to satisfy yourself, and if need be, if we question you ((?)) that you are sending your data to a country with adequate equivalent protection.

Now many countries in the world have that already. Standard contract terms have been devised for that purpose. You mentioned the safe harbour. These have all been attempts to sort of make it easier for organisations, but it's not as easy as it could be, I fully recognise that. That's why I, and a number of my European colleagues, have pushed a lot of weight behind this concept of binding corporate rules, for an organisation to sign up to its own code of practice, written for its own purposes in language which suits its own needs, but recognises the requirements of data protection, and as long as they adopt a code on these lines, then they can export the information without any problems.

We are still trying to make sure that this has universal appeal across the whole of Europe. There's a bit of a north/south divide on this, but we're working in the right direction.

Roger Steel: Thank you. Guy I think a number of us may be somewhat confused in that you said that the legislation was looking for a deterrent effect, but you also said that it was remedies based, and that is the confusion that I have about this particular legislation. Is there any evidence that it has actually achieved its deterrent objective?

Guy Dehn: Yes there is. But can I start by saying, if there was any impression that I'm into bashing lawyers, I'm not. I have no doubt that think the rule of law is absolutely vital in a free society, and you can't have the rule of law without the role of litigation. Lawyers operate in the system and society we provide and when it comes to litigation we expect them to fight the interest of their particular client, irrespective of any wider public interest. All I am saying is that for an individual, I equate litigation with open heart surgery. When you need open heart surgery, boy you need it, and you don't want anything else, but it's not

something that should be undertaken lightly or when you don't need it.

Can I now answer your question. Roger if anyone is confused as to what I was saying about the Act's deterrent effect, I can try and explain my thinking again. The deterrent effect on that greengrocer in a competitive market and the link to the remedy, is that he fears he will lose the customer and this means he will go, in a sense, one step beyond what he has to do. He is careful so if he looks at the onions and thinks "They don't look rotten to me", he's probably not going to argue about it, it's not worth it. If he's thinking this guy / this woman spends £150 a year with me, it's not worth my while. So the fear of losing the customer has a deterrent effect on dealing with that problem.

Now you ask for evidence. Well when we started our work on whistleblowing... I've got to emphasise, I'm not saying that you can really show a cause and effect in an area like this..... but during the 90s there were a lot of serious problems in the National Health Service. There was the misdiagnosis of bone tumours in Birmingham, there was what happened at the Bristol Royal Infirmary, there was Harold Shipman, there were at least three cases of problems with cervical smears, and in all of the main ones, when the public enquiries came, it was made abundantly clear that staff who worked there had been aware of what was going on, and had not been prepared to say anything about it. The one doctor who did at the Bristol Royal Infirmary, lost his job and now practices in Australia.

Now remember that the NHS is our biggest employer, it has over a million people working for it; that we all love, well almost all of us love the NHS; that the consumer risks in the NHS are obviously very serious and if you're working there it's probably every day someone will see something that could give cause for concern.

Now of those 750 cases a year that have come out under the Public Interest Disclosure Act, only a handful have come from the NHS, and none of those have come

out of a major patient safety issues. Since the whistleblowing Act has been in force, there hasn't been, so far, a major patient safety issue. Now I've got to put a really important caveat to that, we do not claim, and I don't want anyone to think that we are claiming, that this is because of the whistleblowing Act. There are a series of reasons, structural changes, legislative changes, perhaps it's got something to do with investment as well in the NHS, but before 1998/99, there was a serious problem in the NHS with very serious adverse affects on patients, and people did not blow the whistle. That is not the position now, the survey...

Roger Steel: It's the case isn't it, that the majority of cases that are brought are actually settled, thereby the employee is happy to accept compensation, happy to accept a confidentiality clause, leaving the employer to carry on doing exactly what he was doing before?

Guy Dehn: No, not at all Roger. The Act has in section 43J the only control in the UK and indeed the only control in whistleblowing legislation presently in the world, which controls gagging clauses, so that a confidentiality clause cannot purport to or be enforced insofar as it tries to stop someone making a protected disclosure.

Roger Steel: Having made the claim and being paid off you then do it through getting them to withdraw that claim, and therefore avoid using a gagging clause.

Guy Dehn: No, no, that's wrong. What Roger is talking about is the making and withdrawal of the legal claim; what section 43J addresses is the making of a protected disclosure, so it's a completely different thing, looking at the whistleblowing and not the right to compensation that results from it when someone is victimised. You cannot, in a confidentiality clause, effectively prevent someone making a protected disclosure as it won't be enforceable. Even after the claim has been settled, even if it is subject to a further gagging clause, Parliament has made it clear that this cannot stop someone making a protected disclosure. Added to this, in the

context of the NHS, there has now been a directive issued, or I think its called a direction, issued by the Secretary of State, that is not voluntary, not recommended, that is mandatory to every NHS Trust that they cannot use confidentiality clauses, which keep secret the sum of money that was paid off or in any way conflict with the Public Interest Disclosure Act. So we're going to see a further shift on this issue in the NHS.

Roger Steel: I would have a number of other questions, I'm very conscious that members of the audience might like to ask questions themselves. I have tried to test, as I say, not necessarily representing my own views or those of my firm, but I have tried to test our speakers tonight on their eloquence. I may or may not have succeeded, and I invite you to have your say. Would anybody like to raise any questions?

If not, I will happily carry on, so please... because I've got lots of things I could ask... the gentleman here in the middle.

Colin Wright: Fellow of the Society, for the want of somebody else to say something. I was interested in a comment right at the beginning about the lack of people or places to tell, or to advise about, what I will call a hazardous incident. A hazardous incident to the company's welfare, to the employee's welfare. In my own business of transport we have, air transport and maritime, something we call the 'confidential hazardous incident reporting program', which allows exactly what it says a, not an anonymous report, but the complainant, the reporter, his identity is kept confidential by the ((chirp?)) by the organisations, who then approach the employer or the transport, or the airline, or whatever, the maritime, in an attempt to resolve that hazardous incident. It's a way of getting around that middle management, which tends to block the information going up.

Most of these reports are gratefully received by the Chief Executives at that level. You know the old line about what keeps them awake at night is not what they know but what they don't know. You know, is there

something like that in other industries? Is there a way through HSE, through the financial services, through law firms to actually have that report investigated and brought forward and done something about?

Guy Dehn: What you've said is exactly right. If you're the chief executive of a company and you're trying to do a good job and something goes badly wrong, one of the first things you're going to say is, "Why the hell didn't somebody tell me about this? Why didn't we pick this up?"

The whistleblowing legislation, if it's used by a company, provides an answer that question. Though it gives no guarantees, it means that you're providing your staff with a safe alternative silence, and there are three things that any sensible employer should do. One is that you need to have a good policy, which is user friendly, isn't defensive, isn't bureaucratic, and isn't just another tick box exercise. Two, you should discuss it with your staff. Three you should promote and re-communicate it to your staff, ideally by posters, which say, "We hope you can raise it with your line manager, if you can't there is this senior person you can raise it with. If you're not sure whether or how to raise a concern, you can get free, confidential advice from Public Concern at Work. If you don't trust us, please go to Information Commissioner, Health and Safety Executive or whatever".

Now one of the great advantages of a very clear message like that is it helps the employer and the employee focus on their accountability, on their core business. If there is one of these few employees who's trying to abuse or misuse the legislation, you're making it very much more difficult for that employee to do it. There's no confusion there between the public interest and the private interest because you're flagging in the regulator early. And usually when someone's trying to abuse the position, what's actually happening is they see there's a problem, they think maybe someone's committing a fraud and they put it in their back pocket, and they wait to use it at a time of their convenience and for their personal interest. That is not in the public interest. Now the Public Interest Disclosure Act, if an employer

will use it, is a very, very helpful tool against that risk of abuse that has existed long before whistleblowing was seen in this new more practical light.

Richard Thomas: Can I add just one word in response to your question, which is, The Freedom of Information Act will fully come into force next year, but many parts are already in force, whereby public authorities now are bringing much more information into the public domain.

If you read Lord Phillips' report into the BSE crisis of a few years ago, his sort of number 2 target was unnecessary secrecy inside Government circles, where people knew what the problems were, but there was no mechanism to bring that into the public domain. So Freedom of Information already is bringing stuff out on a voluntary basis and see change going on across Whitehall departments. As from January they'll be a right of request.

Christopher Norris: I'm a Fellow of the Society, and I also work in U Media. I just want to ask, hopefully, quite a simple question. When, on websites, they ask you to fill out sort of questions about your own personal details and things, are there any restrictions as to what people can ask you, and if so, what kind of redress have you got with people who... you might be subscribing to some, you know, magazine or something from say, the States. You know, what kind of laws are there in cyberspace for these kind of data protection issues?

Richard Thomas: It's a pretty big question, I'll try and answer it in two or three ((?)). In the domestic environment, there's no sort of prohibitions on what can be asked as such in most areas. By and large, you know, it's up to you if you want to use a particular service or buy the particular goods, well if you're happy to volunteer information to get that, you do so, if you don't, you don't volunteer the information.

A bit different in the public sector where data protection and other requirements,

you know, can sometimes limit the amount of information being collected, and I touched on identity cards, that's one of the debates coming up there. How much information should and could be collected on this massive central database?

I fully recognise it does get more difficult to deal with these matters at the international level, but that's why I played so much emphasis on, you know, the international transporter flows the European Union has now got, you know, this interconnected across Europe with, you know, equivalent measures in Australia, Canada, New Zealand, Argentina, Venezuela, you know, there are equivalents.

A little more difficult with the United States, as was mentioned in the previous question, but we work very closely with bodies like the Federal Trade Commission and so on, to try and get a sort of harmonised approach. A cross border enforcement can be more difficult.

I was described in the Daily Mail recently as the 'Spam Buster'. Not a happy title, and under the new privacy and electronic communications regulations, I am supposed to deal with cases of spam, unwanted email. Now 99.99% recurring comes from either Florida or Uzbekistan or elsewhere, very difficult in practice to deal with that, but we're working on it.

Malcolm Aickin: I wanted to tell you a story, but there's a question to both of you in it.

I had a disagreement with a regulator, who I don't particularly want to name because it's now past, who misstated the regulations to a House of Commons select committee, as a result of which I wrote to them and said, "You have misstated the regulations. It seems to me that a statement by the regulator quoted by the House of Commons, will appear to have the semblance of authority and you ought to correct it, and if you don't correct it, then I will have to do so myself", and to cut a story short, I ended up doing so, as a result of which the regulator endeavoured to victimise me.

There are several bits of legislation in existence which protected that, both the contempt rules of the House of Commons and

an 1890 statute, which talks about protecting witnesses at public enquiries, and that you should be treated badly if you endeavoured to damnify them. The thing which is interesting about that particular piece of legislation is that you can seek both civil damages and criminal prosecution in the same case.

The result of that was not that any of those things were followed, except that the select committee did call them back to apologise for their contempt, which they did. The Chief Executive lost his job as a result, and it was all fairly unpleasant.

Both of you have talked about how the bits that you're talking about will enable competitiveness, but that requires that people act in a rational way, that people actually learn by their mistakes.

One of the things which this particular regulator has now done, is to write to all the organisations, whom it regulates and say, "If you have not got a signed statement from all of the directors and managers of your organisation, which say they have not been debarred, say they have not been a member or an organisation, which we have struck off our register, then you're in violation".

Now first of all, that's not what the regulations say. Secondly, they presumably know which organisations they have compulsorily revoked, and they know because they have the right to the information who the senior managers and directors were.

So why are they trying to put this huge burden onto all the organisations whom they regulate. Because they say that the list of people, which they admit to having, they could not release for reasons of the Data Protection Act.

Now it seems to me that if what I did was to try to drive these people towards acting more sensibly in the interests of better regulation that people could adhere to and get the things right. How, in the absence of intelligence, which this seems to be, do either of your bits of legislation and paraphernalia drive people to do the sensible thing, when they seem incapable of doing it?

Richard Thomas: I think I'd better go first on that one. I may need to have a written exchange on this, because I need more detail about the particular circumstances.

There are many examples where, as I said earlier, data protection is blamed for not passing on personal information, which can and should be passed on. There are great provisions in the Act dealing with law enforcement, dealing with regulation, dealing with the proper functions of an organisation, so I'm puzzled now as to why a regulatory body is having the sort of difficulties which you are outlining to us.

I've placed a lot of emphasis on, you know, a sort of, a common sense say, rational approach. I've said that I don't want ever, to see anyone, you know, using data protection or not doing something for reasons which no one could sensibly and rationally justify. You know, there are some restrictions, yes there are, but there is good reason for those, so I can't go into more detail without knowing more about the case, but I am puzzled, but it may not be the first nor the last example brought to my attention of where people feel there are some rather bizarre outcomes attributed to data protection.

Roger Steel: I think it's probably one to take off-line isn't it.

Okay, ladies and gentlemen, we are slightly after our time. Has anybody got anymore burning questions, of course... ah, the gentleman at the back, I'll take that as the last one if I may.

Just to repeat our invitation to join us for a drink in the Benjamin Franklin Room downstairs, if we can take this as the last question. Thank you.

Nick Fenner: From Watson Farley & Williams. A question for the Information Commissioner. Do you have any concerns about the deal that's been struck with the US over the transfer of passenger data?

Richard Thomas: Another very difficult issue. Within the United Kingdom, we are broadly comfortable with what British Airways and other airlines flying out of this

country are doing. They are complying with the requests from the... well the requirements of the US Authorities, who want, not just name and address, but a great deal of information about people's background, including for example, you know, special diets and the onward journeys and so on.

We take the view, first of all, that you know the United States is a sovereign country and is entitled to stipulate requirements of people who are going into that country, and secondly people, to use the language of the Data Protection Act, the information is passed on in fulfilment of a contract, as a contract between the individual and the airline.

So we have not closed down Heathrow Airport, you will be pleased to hear, and the flights are still going. Having said that, we do have some concerns, we think that alongside many of our European colleagues, take a somewhat harder line than we do on this, but we have sort of got a sort of a compromise, consensus position. We, at the European level, think the Americans have been asking for too much information in some cases, and they want to hold it for purposes which are well, well beyond the fight against terrorism.

Originally they wanted to hold the information for, I think it was, 15 years. The French thought 3 days was about right. The deal which has been done is 3½ years, and that's no genius to work out that's halfway between 3 and 4, where the negotiations ended up.

It's a very controversial subject. The European Parliament has been very critical of the European Commission, which struck the deal. There are, you know, a number of data protection authorities who think that the deal is not acceptable. We're dealing with some very, very tricky issues here, but at the moment, you know, we're not taking any active action.

Roger Steel: Okay, well ladies and gentleman, I think there we must leave it. The aim of this evening was to test the question. I suspect our speakers have won the debate, but if you have any further questions to put to

them over drinks, please do so. Thank you very much.