BILETA

16th BILETA Annual Conference

April 9th - 10th, 2001.
University of Edinburgh, Scotland.

Data protection and E-commerce; The case for new law, in the information age.

ANDREW JOHNSON
(University of Edinburgh, UK)

Introduction.

Data protection is not in itself a new concept, (footnote) but has become an increasingly important issue in the digital age. Previously a jurisprudence interest data protection has increasingly become part of the mainstream of the legal debate in part due to e-commerce. Data protection can be defined as safeguards to protect the integrity, privacy and security of data. The focal point of Data protection is that of individual autonomy, the ability to control. However private companies have seen the ease of collecting, collating, manipulating and using data become increasingly easy due to technological advances. E-commerce itself is perhaps the ideal medium to collect the most information in the most cost efficient way about consumers. It is the claims of e-tailers and telecommunication companies (footnote) that this ability to gain information will help these companies to greater understanding of the consumer's needs. However should the law allow companies to use this information as they want? What are the current controls? And what should the law be?

It has long been stated that knowledge is power, now perhaps is the time for this maxim to be revised to Information is profitable. Whilst a single piece of data may be worth little, it is the ability to use and manipulate data to target consumers that e-commerce regard as an advantage. E-commerce has seen private companies collect and collate data on a scale previously reserved for governments.

This leads to a potential conflict, business sees information as essential for profit. Consumers though are concerned about who has information about them, and how they collected it. This in part can be reflected by the recent legislation of the European Union (pro-individual), (footnote) and the lack of regulation by the United States (pro-business.) I aim to show though that the European Union is pro-business and the stance of the United States may be damaging in the long run to E-commerce.

Many people including those involved in e-commerce and those looking in from the outside say the key to increasing the number of people using e-commerce is a matter of trust. Therefore if e-tailers increase the protection of your everyday data e.g. your e-mail address you are more likely to trust them with your credit card details. Thus an e-tailer which has a very strict data-protection regime may see their orders increase. Likewise a business with an ineffective data-protection programme may see their business suffer (Barclays footnote). Businesses instead of being anti data-protection should instead be embracing it, however for this to happen the case in favour of data-protection

needs to be made once more. This is my aim.

Data Protection.

Data protection/privacy should in principle be based around the maximum control for the individual (information self-determination). Data protection is an ideal idea, and it is unclear what it is. It indicates a direction rather than a specific level. Data protection can not be fixed but rather alters as society values change. The integrity perspective interacts with a protected private sphere, the closer you get to this private sphere the stricter the law should be.

Data protection is used as the basis for decisions, not only formal decisions but also other decisions. This can include video surveillance in a shopping mall, where young people could be asked to leave due to bad conduct. The basis for these decisions is very important, and the use of technology has the power the change the classical structure between business and consumers. Thus due to the information imbalance the consumer may be tricked into buying a product. The business may have a detailed customer profile built up and either use that themselves, or alternatively sell to other businesses who can target you as a consumer. This leads to an imbalance of power.

It is these principles which after much debate and problems finally resulted inthe European Directive on Data protection (footnote)

The Data Protection Directive and the Data Protection Act 1998 (need to talk more about DPA 98)

The present law with regards to data protection in all EU and EEA member states is based on Directive 95/46, The protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive has created new obligations for those who process personal and has created new rights which individuals can enforce to make sure that there data is not misused. One of the aims of the directive was to introduce a common standard of data protection throughout the EU to enable the free flow of personal data within the EU, thus strengthening the single market. The Directive also provides for a system that will recognise the equivalent standards of data protection in a third country enabling the transfer of data outside the EU. (footnote)

Aims of the Directive.

The Directive focuses on the individuals right to privacy. It applies where any information relating to an identified or identifiable natural person (the "data subject") is processed (footnote) wholly or partly by automatic means and by non-automatic means where the data are part of a filing system. The Directive includes five data quality principles that the data controller (footnote) must comply with. The data controller must ensure that personal data is:

* Processed fairly and lawfully;

* Collected and processed for specified, explicit and legitimate purposes;

* Adequate, relevant and not excessive in relation to the purposes for which it is collected;

* Accurate and kept up-to-date where necessary; and

* Kept in a form that allows identification of individuals for no longer than necessary in view of the purposes of the processing.

Increased rights of the data subject.

The general rule is that the data subject must give his consent to the processing of personal data.

(footnote article 7 and 8 (Special categories of processing) maybe an appendix.) The data subject will also be able to object on `compelling legitimate grounds' to data about him being processed. In these instances though, the issue will focus on the balance of the legitimate activities of the business against the rights of the individual. It therefore requires businesses if challenged, to demonstrate that their activities are legitimate. (Check how this has gone in the DPA 1998, and also research, how many people have complained to the data com, Against which companies (look in annual report) This is useful for later to back up argument for new law. Is it merely a case of a business being able to say that we needed all this info on customers to provide a better service/ market profile / sell more stuff/ or will the body have teeth and back up the consumer (unlike the comp. authority).

The data subject should also be able to obtain information from the data controller with regard to his identity and the purposes of the processing of data relating to the data subject. However this is only to the extent necessary to guarantee fair processing having regard to the specific circumstances in which the data is collected. (check the DPA 1998) If the data has not been directly obtained from the data subject, the obligation to inform will not apply where this would be impossible or would involve a disproportionate effort. It is unclear how this would work in E-commerce, if we consider email addresses, which had been obtained through a third party should the data processor contact the people through e-mail to ask for their consent. Or if they have given their consent to the third party, in a form which states that this data may be passed onto third party's have they already given there consent. This is unclear, at present it would seem that if the data subject had willingly consented knowing that his data was going to be transferred to a third party then that third party is under no obligation to contact them. However this raises the matter of consent. Unlike many other forms the data protection aspects on the on-line form are not prominent (often at the bottom of the form) and often complicated. In the real world the data protection notice is often next to signature line, and prominent. Although the online world may be necessary in some aspects due to its very nature, this aspect could and should be altered. (footnote from data protection authority) Also waiting for a response from a number of e-mails sent including ones sent to the data protection commissioner

In addition to the right to information, the data subject is entitled to have access to the data and have the data rectified or erased if incomplete or, inaccurate or if the processing otherwise infringes the Directive. The controller must notify any rectification or erasure to third parties to whom the data have been disclosed unless this proves impossible or would involve a disproportionate effort. For a good example perhaps include the Mark Thomas comedy product.

Direct Marketing

Direct Marketing is dealt with specifically under the directive. This is perhaps one of the most important areas of the directive with regards to e-commerce. However it has also resulted in the aims of the directive, that of a unified European Union stance with regards to data protection thrown into doubt. The directives key requirement is that the data subject be able to object to personal data relating to him or her being processed for the purposes of direct marketing or to be informed before the personal data is used for direct marketing. The UK government (DPA 1998) has resolved this issue be allowing data subjects to object by signing a opt-out form to their personal data being used for direct marketing purposes. It is not specified if it is possible to circumvent this right to object by obtaining the data subject's consent when the data is originally obtained. This though raises the question of imbalance of power and once more calls into question if the consent of the data subject was really genuine or not.

However one of the main problems, in the directive was the general wording with regard to Direct Marketing which has resulted in member states implementing it in slightly different ways. Thus in the majority of States (generally those with the originally more laissez-faire approach to data protection) we have an opt-out system. Whilst in four member states (where historically data-protection has been seen more as a semi-quasi human right) we have an opt-in system. This results in a major difference in the result of direct marketing for e-commerce companies using e-mail to target

customers. Whilst this clearly undermines the directives aims of creating a single European stance on data protection, for an e-commerce firm in operating in all of Europe the problems may be smaller than imagined. This is mainly due to the differences in language, whilst you may be able to advertise in maybe one or two languages, it is more effective to advertise in the native language. Thus whilst it may be more difficult for an e-commerce firm it is not the end of the world.

Remedies

Individuals will be able to have a judicial remedy for any breach of the guarantees provided by the directive. If a data subject has suffered damage due to the result of an unlawful processing they will be entitled to receive compensation from the controller. However the data controller can avoid liability if they are able to prove that they are not responsible for the events which resulted in the damage. Member states must also provide a system which enables sanctions to be imposed in case of violations. A controller who fails to comply with national laws implemented stemming from the directive may find themselves liable to be sued for damages and prosecuted by the data protection commissioner.

The EU V USA Not so different after all ?

(check for internet argument that claims that the EU and USA position is in fact much closer and more similar than many other academic writers argue.)

The free movement of data can be very useful. For instance if you are going on holiday the information about your flight and hotel reservations can be recorded in the hotels data base, including your credit card details. You become ill and therefore they require your medical record and your insurance company is also contacted. In two years time you return, but immigration refuse you entry to the country as you have a very rare disease. This example shows the benefits of the system, but also the possible negatives.

Law is required in order to regulate the movement of this data. With the single market there is free movement and it is necessary for the movement of personal data for travel and work. One of the main problems is the requirement of free movement with the protection of data. This has been dealt with by the E.U. Data protection Directive 95/46 EC became effective on October 25, 1998. Which allowed the free transfer of data within the EU but prohibited the transfer of personal data to a third country, unless that third country provides an`adequate' level of protection for that date. (footnote Article 25)

On of the problems here is the potential impact on E-commerce, in part this has been resolved by the Safe harbour agreement. This now enables the transfer of data between the EU and the USA, it does highlight the difference between the two regimes underlying principles. The USA favouring in part self-regulation and legislation compared to the E.U.'s use of legislation.

The organisation must give the individual clear details about the information it is collecting, how it will use this information, to which it will disclose the personal data, how to complain and who to contact. The individual will be able to opt-out to their information being transferred to a third party, unless it is sensitive information that requires an opt-in for transfers or alternate uses. Once more this could result in confusion for both the e-commerce business and the public, perhaps an opt-in system should be adopted throughout the E.U,and the USA. This would remove any possible problems with regards to consent, it would also redress any possible imbalance between consumers and business.

An organisation can comply with the safe harbour in a number of ways. This can include joining a recognised regulatory scheme, such as TRUSTe (footnote with examples of the failings and recent case examples). However the strength of these provisions must be called into question, by their very nature they lack the same enforcement strength as hard law. We will have to see if they do actually

provide the safe guards the E.U require them to do. This author would have doubts about the adequacy of data protection in the USA, especially when it comes to enforcement. However I aim to show that it would be beneficial for e-commerce firms to strictly enforce data protection requirement, be they voluntary, or a legal necessity.

Data protection and E-commerce; compatible ideas?

One of the main issues concerning E-commerce, is that of trust. In this respect data protection has an important role to play. Strong data protection should increase consumers trust in the Internet and as such lead to an increase in e-commerce.

This is reflected in a survey, which Harris International carried out with 3,000 customers for IBM in the USA, Great Britain and Germany. (Hoping to arrange a meeting with IBM to discuss the survey and future impact on e-commerce.) In all three countries customers felt that their data should have the highest degree of protection when shopping on-line. Thus the expense of providing a strong data protection could be off set by the increased demand in business which would be achieved.

The IBM multinational consumer privacy study was able to show that companies which clearly formulated their privacy policy and, made it transparent enjoy advantages with customers. Furthermore on-line customers with a good education, technical knowledge and a higher income saw data protection as very important.The group of people which many e-commerce businesses want to attract. Around 50 percent of British and American people questioned requested an explanation on the website about the use of their personal data. 63 percent of the people questioned would not be willing to disclose their personal data on a website that does not guarantee data protection. Perhaps the most important statistic for e-commerce is that 40 percent declared that they would not purchase an item from that e-tailer if they had fears about the misuse of data for online purchasers.

IBM draws the conclusion that customers have less trust in the handling oftheir data than the providers of online services realise. If this survey hadonly been conducted in Germany and Europe, I would not have been surprised atthe results, however the use of the UK and the USA, in part reflect the changein public opinion and their attitude towards data protection. It would seemfrom these results that an e-commerce firm would have an advantage over theircompetitors if they reflected the consumer's desire of stronger data protectionof their data. Whilst the cost of implementing stronger data protection(especially in Europe following Directive 95/46) (footnote on cost so far ofimplementing the directive) may be a worry, it would seem that the increase inbusiness would off set any additional costs.

E-marketing and Data protection.

One of the areas in which e-commerce firms feel they have an advantage over real world firms is the cost of marketing. However this is perhaps one of the most annoying aspects of the web, and an area which e-commerce firms should think twice before pursuing an aggressive e-mail led marketing campaign. It is also an area where a number of States of the USA have implemented laws, and the EU has produced a number of directives that cover these areas.

The development of e-commerce has also seen an increase of concern regardingthe unlimited harvesting and uncontrolled commercial sale of personal data, thecreation of vast databases of personal profiles, aggressive advertising, increasing use of unfair practices and serious infringements of privacy. The European commission has responded by producing a report on Unsolicited Commercial Communications and Data protection. It focuses on "spam" and raises a number of interesting points, some of which I will aim to show create or may be more accurately represent conflicting principles which are present in IT law.

A development in e-commerce is the increasing use of new permission based e-mail marketing strategies which are now being practised world-wide by a number of leading e-commerce players. In part this is down to the cost advantages, e-mail marketing is perhaps the only form of marketing in which the cost of the recipient is greater than that of the sender.

There are perhaps two central claims behind new permission based e-mail marketing strategies, claims which Serge Gauthronet and Etienne Drouard do not challenge, but I will. The first is that of consent, in a permission based system data is gathered by the use of an opt-in form on a website, which in return will give a benefit (footnote) to the data subject. These services are free in return for there e-mail, which is then placed on a main data base. This way of collecting data is legitimate, however I would question anything whichis an exchange of information, as there is no such thing as a free lunch. This in my mind calls into question the matter of consent without these inducements would the data subject have submitted their e-mail address. Although I lack evidence my suspicion is the majority of people would not submit their e-mail address. It is estimated that around 20 million e-mail addresses are currently stored, with the number increasing daily. Although legitimate, and whilst the consent is genuine, I feel it is not a complete meetings of equals.

A further claim by the e-commerce community is that gathering this data enables customers to be targeted more effectively. This however is a spurious claim, as it is the company which decides who to target, not the consumer. I may be an occasional shopper on a website, and in the real world I would visit the shop when I needed something. With e-commerce I may receive many targeted adverts a week.

Perhaps the most interesting aspect of e-commerce and direct marketing is the claims of it being personal to you. This is called customer core marketing and B.T is involved with it, The Times newspaper also supports it, however it has anumber of flaws. The aim is to develop a relationship, it seems strange that e-commerce firms espouse the benefits of a personal service whilst with cases of libel the defence is often that the comment would not have been made if it had not been on e-mail, as it seems so remote. This is an interesting conflict, in one instance you can attempt to raise a defence that e-mail is an inherently impersonal system, whilst at the same time claiming it is the break through for customer relationships. The claim is that it enables multinational businesses to treat you like the local village shop keeper does. However this is a false claim, to have an e-mail from amazon.co.uk addressed to Andy, is not personal in fact it is the reverse. It reminds me of walking by a conference building when the delegates where leaving, I was able to approach them and call them by their first name and greet them as friends due to their name badges. Now whilst most responded it was almost always with a degree of suspicion, this is often the impression direct marketing by e-mail gives. They do not know me, but rather have used a simple computer programme to appear to know me.

An extreme example of this may be an on line e-tailer who is able to monitor and process data. They may notice that a female aged 29 has stopped buying sanitary products, after nine months they then send an e-mail advertising there baby products. However she may have miscarried or had cancer, something which a local village shop keeper might know, but a on-line e-tailer has no hope of knowing. This is the inherent problem in this system and something which all firms in e-commerce should take into account. It is not possible to and nor should it be allowed to target customers in this way, and not cause offence and bad publicity in certain circumstances. The same also occurred in the realworld with M & S check example.

It should be made clear though that the collection of e-mail addresses frompublic spaces on the internet is in breach of the principles of fair collection(Article 6.1(a) of Directive 95/46/EC), finality (Article 6.1(b)) andlegitimate processing (Article 7(f). The policy of the European Union is that the senders of commercial e-mails should be required to obtain the prior consent of the addressees.

Is opt-in now the norm ?

With a number of EU countries adopting this approach in National legislation,which implemented Directive 95/46 and many e-commerce firms following thisroute for business purposes, is it now the time to make opt-in the standard form. Whilst it may have certain problems (discussed above) it is beneficial when compared to the opt-out format.

However one aspect which raises a number of concerns is the fact that, data collected with the consumers prior consent, can be sold to third parties. It is this which may result in direct marketing becoming as annoying as Spam,especially if the data subject does not realise when they are consenting, that they are consenting to there data being transferred to third parties. Many people will feel that they are opting-in for a service, not for there data to be collated and disseminated to third parties. However it would reduce e-commerce firms using indiscriminate marketing to an extent, yet it would surely depend on which third party the data is transferred to. Thus the business may not be targeting a willing audience. However the data subject will be able to ask to be removed from this list, but if it has been collected by a third party and sold to a number of different businesses, how many times will the data subject have to be asked to be removed from the list. One of the main advantages and disadvantages of the Internet is the speed in which data can be transferred.

Perhaps what is required is for e-commerce firms to seize an economic opportunity and collect information about their customers themselves, and once collected use a very strict data protection regime and not pass data on to other third parties. This would prevent any unwanted direct marketing and also build up trust between the consumer and your on-line business. Whilst the business would loose money which it might have gained from selling its collected data, this will more than be recouped by the increase in revenue from customers who use your e-commerce business as their first choice.

Perhaps discuss the law in greater detail with regard to direct marketing as this is perhaps the most essential aspect of e-commerce at the moment. Thus the earlier section may be moved and altered significantly, in part as I think it could be a much better section.

As the one of the main principles behind the Europeans Unions data protection legislation is the greater the threat to privacy the greater the level of protection. However it seems that the e-commerce directive has not fulfilled this principle with regard to unsolicited e-mail. The wording could and shouldhave been more precise. This has now resulted in a number of states in the United States having stricter laws with regards to spamming, in certain states it is a criminal offence. Whilst Europe is left with two conflicting systems that of opt-in or opt-out lists. However moves are in place to alter this, to provide a technically neutral response (check OJ COM (2000) 385, of 12 July200. Important) Direct marketing revolves around the concept of consent inDirective 95/46, already discussed, but check also I think it reads altering,as does a lot of the essay, this will be re-structured heavily whilst the ideas will remain the same.

Consent is a very important issue with regards to e-commerce and the prospectsof e-commerce growth will be damaged if prospective web shoppers are left in doubt as to the honesty and fairness of online traders.

The approach of Switzerland

New law or regulation

Conclusion.