Bankrupt e-businesses and e-consumer protection

by

Michael Bernhard Boll

Submitted to the University of Exeter as a dissertation towards the degree of Master of Law by advanced study in International business law, September 2004.

“I certify that all material in this dissertation which is not my own work has been identified and that no material is included for which a degree has previously been conferred on me.”
Abstract:

This dissertation outlines the problems the legal systems of the United States of America, the European Union (using the Federal Republic of Germany as an example) have with the protection of privacy interests of e-costumers in the case that the online retailer files for insolvency. It is worked out how these interests are protected and what kind of other interests may oppose the privacy interests of e-costumers. In the following the two different approaches on consumer protection of the US legal system and the German legal system are compared. The problems arising from an interaction of these two different systems are outlined and the solution of the “Safe Harbour” agreement is discussed.

At last a method of resolution is proposed how the gap between the self-regulatory approach of the USA and the governmental approach of the European Union and especially of the Federal Republic of Germany can be filled. Also is a method of resolution outlined how the US approach of e-consumer data protection in the case of a bankruptcy of the e-retailer can be improved.

Word count: 16,434 words
1. Chapter 1 – Introduction ........................................................................................................5

1.1 Data collection: “e-business” v. “bricks and mortar” companies ..................................6

1.2 Bankruptcy: “e-business” v. “bricks and mortar” companies ......................................8

2. Chapter 2 - Development in the United States ..................................................................9

2.1 Toysmart.com judgement on the sale of e-consumer data to a third party ..................9

2.2 Characterisation of individual identifiable information by the Bankruptcy Act ..........13

2.2.1 The Bankruptcy Act and e-consumer data .................................................................14

2.2.1.1 Solution according to Section 365 .....................................................................15

2.2.1.2 Solution according to Section 363 .....................................................................17

2.2.2 The planned Leahy-Hatch Amendment ..................................................................20

2.2.3 Conclusion from the US Bankruptcy Code point of view .......................................23

2.3 Characterisation of individually identifiable information by academics ..................24

2.3.1 The property approach .............................................................................................25

2.3.2 The ex ante contractual approach ..........................................................................29

2.3.3 The ex post viewed tort approach ............................................................................31

2.3.4 The combined approach ..........................................................................................32

2.3.5 Solution of the problem of defining data in an bankruptcy .....................................35

2.4 The Privacy Law ...........................................................................................................39

2.4.1 Gramm-Leach-Bliley Act of 1999 ...........................................................................40

2.4.2 COPPA .....................................................................................................................41

2.4.3 Conclusion Data Protection Law ..............................................................................42

2.5 Conclusion from the United States point of view .......................................................44

3. Chapter 3 - Approach of the EU legislation and further development .........................48

4. Chapter 4 - National laws on e-consumer protection in an insolvency in the EU ..........52

4.1 Characterisation of individually identifiable data in Germany - alienability ..........53
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2 German Bankruptcy Code</td>
<td>54</td>
</tr>
<tr>
<td>4.3 Germany’s approach from the privacy law point of view</td>
<td>56</td>
</tr>
<tr>
<td>4.3.1 German lex generalis on privacy</td>
<td>57</td>
</tr>
<tr>
<td>4.3.1.1 The use, lease or sell of personal data</td>
<td>57</td>
</tr>
<tr>
<td>4.3.1.2 The rights of the affected person and claims for compensation</td>
<td>59</td>
</tr>
<tr>
<td>4.3.2 Special laws protecting privacy</td>
<td>60</td>
</tr>
<tr>
<td>4.3.3 Conclusion Data Protection Law</td>
<td>62</td>
</tr>
<tr>
<td>5. Chapter 5 - Legal conflicts that can arise from an interaction</td>
<td>63</td>
</tr>
<tr>
<td>6. Chapter 6 - Conclusion and method of resolution on the outlined problem</td>
<td>65</td>
</tr>
<tr>
<td>Annex I – Texts of some Laws and Statutes used</td>
<td>78</td>
</tr>
<tr>
<td>§ 361. Adequate protection</td>
<td>78</td>
</tr>
<tr>
<td>§ 363. Use, sale or lease of property</td>
<td>79</td>
</tr>
<tr>
<td>§ 365. Executory contracts and unexpired leases</td>
<td>80</td>
</tr>
<tr>
<td>SEC. 231. PROTECTION OF NONPUBLIC PERSONAL INFORMATION</td>
<td>81</td>
</tr>
<tr>
<td>§ 103 Choice of the receiver – German Insolvency Code</td>
<td>81</td>
</tr>
<tr>
<td>§ 153 Statement of assets and liabilities – German Insolvency Code</td>
<td>82</td>
</tr>
<tr>
<td>§ 4a Consent – Federal Data Protection Code</td>
<td>82</td>
</tr>
<tr>
<td>§ 7 Compensation – Federal Data Protection Code</td>
<td>82</td>
</tr>
<tr>
<td>Annex II – Definitions</td>
<td>82</td>
</tr>
</tbody>
</table>
"It's amazing to see a start-up get $100 million in financing and then when the robe gets taken off, there's nothing. What do you have a lot of the time? The domain name, a little bit of capital, and the crown jewel: the customer database."

Keith Shapiro in Nicholas Morehead “Toysmart: The Bankruptcy Litmus Test, Wired, July 12th 2000

1. Chapter 1 – Introduction

This dissertation shall describe the different developments of the European legal system, especially the German system, and the system of the United States of America dealing with bankrupt e-retailers and consumer privacy issues. It shall deal on one side with aspects of protection of consumers who use the new technologies to order products. And on the other side it shall deal with the aspects of bankruptcy codes that protect the creditors interests when a company files for insolvency. The interest of the creditor is the interest to get back the money or other assets he gave to the bankrupt debtor. One of the key interests of the e-consumer is that his data, collected by the insolvent e-retailer, is not sold to someone else (e.g. to a company that is going to use the e-mail addresses and profiles for unsolicited e-mails, so called spam e-mails).

In the introduction it is going to be explained why new approaches on consumer data protection and bankruptcy issues have to be made. In chapter two the

---

1. [http://www.wired.com/news/business/0,1367,37517-2,00.html](http://www.wired.com/news/business/0,1367,37517-2,00.html) (last visited 4th August 2004), Keith Shapiro is attorney with the firm Greenberg & Traurig and was President of the American Bankruptcy Institute.
system of the United States of America shall be described and the problems arising shall be outlined and discussed. In the third and fourth chapter the system within the European Union and the German system shall be described and discussed. This is followed by an analysis of cross-border problems. There the problems of the interaction both systems are going to be worked out. Finally a method of resolution to these new problems shall be described.

1.1 Data collection: “e-business” v. “bricks and mortar” companies

In the beginning it shall be outlined if there is significant difference between the new e-business and the common business of “bricks and mortar” companies as initial prototype of the retail business. These so called “bricks and mortar” companies have catalogues and offer their products in the way of distance selling. Secondly it is going to be researched if do we really need new laws for the “new economy”. Dealing with the first mentioned issue the common retailers collected only data of their costumers when their costumer orders products. The data usually was limited and comprised only of the products ordered, the shipping address and the details of payment.

E-retailers do collect a by far bigger amount of data dealing with their e-customers. With a so-called “cookie”\(^2\) the e-retailer is enabled to collect data from its customers and even of visitors who they only viewed the homepage once. This happens even on the first visit no matter if the e-consumer orders an

\(^2\) For an exact definition see Annex II “cookie”.

article or not. The cookie allows collecting data concerning the behaviour of the e-consumer in the Internet (e.g. which pages is the consumer using and how long is he on these pages, does he order from other e-retailers and how often does he so; which type of products does the costumer prefer and with which system does he pay?). This huge amount of data collected by the e-retailer gives a detailed profile of the Internet user and costumer. This leads to a by far more detailed database than any “bricks and mortar” company can collect. This kind of data is usually called “individually identifiable information” or “personally identifiable information” in the US jurisdiction and academic articles. This kind of information is defined as “[information] that can be used to identify an individual, that is elicited from the individual by the company’s web site through active or passive means, and that is retrievable by the company in the ordinary course of business.” The amount of data and the very detailed profile gained from this is the reason why e-retailers are different from “bricks-and-mortar” retailers. A different treatment with special privacy rules is not to be introduced because the common retailers also entered the e-business or bought consumer data from so-called data miners. This blurs the clear-cut borders between the old economy and new e-business and makes special laws for e-retailers obsolete. But through the Internet and the appearance of e-retailers the things have changed and the collection of data has changed in a very drastic way. The amount of data

---


collected and the storage over a long period of time of costumer data can result in a complete profile of the costumer and the costumer’s family. All these facts made a new data protection law necessary. In the 1990’s and in the new millennium the USA and the EU framed new privacy laws. It is going to be worked out if the new data protection law in the United States and the European Union can protect the interests of its citizens – the e-consumers.

1.2 Bankruptcy: “e-business” v. “bricks and mortar” companies

It has also to be researched, if the current Bankruptcy codes still live up to the expectations to satisfy the creditors and to protect the warrantable interests of the e-consumers.

Dealing with bankruptcy aspects a distinction can be made between “bricks and mortar” business and the dot-com business, too. The first mentioned have usually more tangible assets (e.g. equipment, fixtures and inventory) that can be sold and thus the creditors can compensate some of their interests. An e-retailer usually has not as many tangible assets (e.g. some computers, bureau equipment) as a “bricks and mortar” business. It usually posses lots of intangible, intellectual property based rights on web-designs or specially tailored software for the database. The costumer’s database is one of these intangible assets. It usually contains such data as name, age, gender, e-mail address, additional information gained by the use of cookies, order forms, surveys etc. may be an asset of special interest. Not the raw data itself, but especially when it is analysed, it can give a very precise profile and enable the user of this data to predict the e-customers
future habits. This type of intangible assets could be used in an insolvency procedure when a dot-com business files for bankruptcy.

The first jurisdiction that had to deal with this problem of the aforementioned conflicting interests of the creditors and the consumers was the jurisdiction of the United States of America. In that country many Internet companies filed for involuntary insolvency in 2000.

2. Chapter 2 - Development in the United States

The jurisdiction of the United States of America is the most developed one on cases dealing with the bankruptcy of e-businesses and the protection of the e-costumers. In 2000 when the new economy bubble burst the first companies filed for an insolvency procedure. Several insolvencies were filed under Chapter 11 of the Bankruptcy Act like DrKoop.com, and living.com. Some companies like craftshop.com tried to sell their costumer lists in its insolvency procedure in May 2000, but opted not to sell after the Texas Attorney General’s Office challenged the sale. The most important case of these years was Toysmart.com as case of precedence.

2.1 Toysmart.com judgement on the sale of e-consumer data to a third party

Toysmart.com collected detailed personal information about its costumers and visitors. This data included the address, billing information, shopping

---


7 Ibid.
preferences, and family profiles. The company collected some of this data from children on its web site through a dinosaur trivia contest.\textsuperscript{8} Also they collected data from the customers. All these family profiles contained inter alia the names and dates of birth of the children. Toysmart.com has had a strict privacy policy and was approved by TRUSTe.\textsuperscript{9} This company reviews and validates the privacy policy. If the e-retailer complies with the standard set up by TRUSTe, the e-retailer is allowed to display the seal of TRUSTe on its web site. Since September 1998 the company posted the following privacy policy on its web site: \textit{[Personal] information, voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared.}

\ldots

\textit{When you register with Toysmart.com, you can rest assured that your information will never be shared with a third party.}\textsuperscript{10}

Toysmart ran into financial problems and ceased its business to consumer operations on May 19\textsuperscript{th} 2000. It tried to reorganise the business with a plan to operate as business-to-business retailer and hired the Boston based “The Recovery Group”.\textsuperscript{11} This group should locate parties interested in acquiring the company’ business and assets.\textsuperscript{12} On the 8\textsuperscript{th} of June 2000 Toysmart advertised to sells its customer data in the Wall Street Journal.\textsuperscript{13} In the following time Toysmart.com L.L.C. was forced by its creditors to file a Chapter 11 bankruptcy

\begin{footnotesize}
\footnotesize
\begin{itemize}
\item \textsuperscript{8} FTC v. Toysmart.com, LLC et al., to be found at www.ftc.gov/os/2000/07/toysmartcomplaint.htm (last visited 28th July 2004).
\item \textsuperscript{9} See Annex II “TRUSTe”, www.truste.com.
\item \textsuperscript{10} http://www.ftc.gov/opa/2000/07/toysmart.htm (28th July 2004).
\item \textsuperscript{11} http://www.ftc.gov/opa/2000/07/toysmart.htm (28th July 2004).
\item \textsuperscript{12} http://www.ftc.gov/opa/2000/07/toysmart.htm (28th July 2004).
\item \textsuperscript{13} Farah Z. Usmani, op cit. at FN. 6.
\end{itemize}
\end{footnotesize}
case on June 9th, 2000. Ten days later the bidding for Toysmart’s assets concluded. On July 10th the Federal Trade Commission (FTC) filed a complaint seeking to permanently enjoin Toysmart.com from selling its list of customers. The FTC made clear that it expected a violation of section 53 of the FTC Act and COPPA (the Children’s Online Privacy Protection Act of 1998). In July 2000 the FTC and Toysmart.com reached a settlement in which the parties agreed not to sell the database in an auction to the bidder that makes the highest bid, but to a company that is a “qualified buyer”. This company shall also act in the same business sector like the defendant did. Also the ”qualified buyer must abide by the terms of the Toysmart privacy statement. If the buyer wishes to make changes to that policy, it must follow certain procedures to protect consumers. It may not change how the information previously collected by Toysmart is used, unless it provides notice to consumers and obtained their affirmative consent (“opt-in”) to the new uses. This solution was not found unanimously. The settlement was opposed by two of the five FTC officials. These officials claimed that the consumer data was not protected as well as possible. Namely Commissioner Swindle stated in a dissenting opinion that the FTC should not have allowed the sale. He stated:

15 15 USCA § 53.
16 15 USCA §§ 6501 – 6506.
18 http://www.ftc.gov/os/2000/07/toysmartconsent.htm (28th July 2004). 4. “Qualified Buyer” shall mean an entity that (1) concentrates its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction, including commerce, content, product and services, and (2) expressly agrees to the obligations set forth in the Stipulation and Order Establishing Conditions on Sale of Customer Information, entered by the Honourable Carol J. Kenner, Bankruptcy Judge for the United States Bankruptcy Court for the District of Massachusetts, in In re: Toysmart.com, LLC, Case. No. 00-13995-CJK (the “Bankruptcy Order”)
[Toysmart] promised its customers that their personal information would never be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because “never” really means never.”

Next to the two officials forty-six Attorneys General opposed the settlement proposal of the FTC because the settlement violated the privacy law of these forty-six States.

The objections of the States regarding the settlement and the settlement itself turned out to be irrelevant because the Bankruptcy Court refused to accept the proposed settlement. The Court redrafted the settlement, but there was no final judgement made by the Court. In the end Buena Vista, a subsidiary of the Walt Disney Co., that was a 60% shareholder of Toysmart.com subsequently acquired the database for 50.000,- $ with the approval of the District Court and destroyed the database. These proceedings brought up all the problems and possible solutions of customer databases in the new economy. The purchase of the database and the destruction by the major stakeholder of Toysmart.com was more or less a public relations action by the Walt Disney Company.

This insolvency proceeding revealed several questions. These questions can be put into different groups. The first group is dealing with the characterisation of individually identifiable data in an insolvency procedure. How has a database of individually identifiable data to be treated in insolvency proceedings? Is it intellectual property or can it be characterized as contractual obligation between

---

the e-consumer and the insolvent e-retailer? What kind of solution is offered by the US Bankruptcy code and what kind of solution is given by the academics? The second group of questions arising from this are dealing with privacy law aspects. If it is possible to sell the database, which of the three possible options does the insolvent e-retailer have? Can the company sell the database without any consent of its customers or are “opt-out”-systems or “opt-in”-systems more suitable for the company and the customers?

2.2 Characterisation of individual identifiable information by the Bankruptcy Act

At first it shall be outlined which approach the federal legislation took to solve the problem of individual information in an insolvency proceeding. An e-retailer has some choices for the disposition of its assets when a financial crisis is coming up. The following are the most important choices: The reorganisation or liquidation bankruptcy of the company according to Chapter 11 proceedings of the Bankruptcy Act. Other choices are the liquidation bankruptcy according to Chapter 7 of the Bankruptcy Act, or a merger with a financially stronger partner; liquidation outside the Bankruptcy Act, asset sales or cessation of operations and abandonment of the business.21

This reorganisation law of Chapter 11 gives some indications how individually identifiable information can be treated. There are two different approaches discussed to find a solution how this type of information can be treated under the US Bankruptcy Code. One approach is made under the current Bankruptcy Code

---

according to Section 365 and treats the individually identifiable data as a kind of contractual situation, there were similar cases decided in the “off-line” world. Also this data can be treated as property of the estate according to Section 363 of the Bankruptcy Code. “Property” shall be defined in this dissertation as any interest in an object, whether tangible or intangible, that is enforceable against the world.  

22 “Contractual obligations” can be defined as relation that only binds the parties in privity.  

2.2.1 The Bankruptcy Act and e-consumer data

Unfortunately for e-consumers, bankruptcy law is not used to provide adequate protection for privacy interests. There is until today no provision in the Bankruptcy Code to protect privacy issues. The closest is a section that intends to protect the public from scandalous matter and the debtor from loss of secrets.  

24 There are only the common rules, which may also protect privacy without explicitly referring to it.

First of all the mechanisms of an insolvency procedure have to be made clear and afterwards the aforementioned problem has to be discussed. According to the US Bankruptcy Act the filing for insolvency triggers automatically a stay of proceedings in respect of all obligations of the company.  

25 The automatic stay prohibits any action taken to perfect or otherwise enforce a lien after the insolvency is filed. It is intended to protect the assets of an insolvent company

---


23 Henry Hansmann, Reinier Kraakmann, op. cit. At FN. 22.

24 Title 11 USCA Chapter 11 § 107(b).

25 Title 11 USCA Chapter 11 § 362 (a)(4).
and thus to protect the interests of the other creditors. When a company has filed for insolvency all the assets are transferred into the “property of the estate” of the insolvent company, which is automatically created. A trustee is also installed to safeguard the distribution of the assets.\textsuperscript{26} The estate of the insolvent company includes the pool of assets that will be finally distributed to satisfy the claims of the creditors. The Bankruptcy Code broadly describes the definition of the “property of the estate”. It is stated that it comprises all of the insolvent company’s interests in its property, wherever located, including proceeds of or from the property of the estate.\textsuperscript{27} One of the centre doctrines of the US Bankruptcy Code is the respect of property rights created under non-bankruptcy. It is still not clear how customer data can be treated in an insolvency procedure. According to the Chapter 11 bankruptcy proceedings there are two approaches possible to find a solution to the problem of the treatment of customer data.

2.2.1.1 Solution according to Section 365

In line with the first solution, individually identifiable data can be treated according to Section 365 of the Bankruptcy Code. The treaty of dot-coms with TRUSTe or the let of the data itself under the terms and conditions not to sell the data can be treated as executory contract and can be rejected under Section 365 of the Bankruptcy Code.\textsuperscript{28} In this case individually identifiable data is treated as contractual obligation.

\textsuperscript{26} Title 11 USCA Chapter 11 § 541.
\textsuperscript{27} Title 11 USCA Chapter 11 § 541 (1)(a) defines estate as “[all] legal or equitable interests of the debtor in property as of the commencement of the case.”
\textsuperscript{28} See Annex I.
This can be concluded from Title 11 USCA Chapter 11 §365 in the actual version amended in the year 2000, which permits the trustee to assume or reject any executory contract or unexpired lease of the debtor. Unless the Bankruptcy Code does not define the term “executory contract.” Professor Vernon Countryman tried to define it in the early seventies of the last century.\(^{29}\) According to the Countryman definition an executory contract is a kind of contract under which “\textit{[the] obligation of both the bankrupt and the other party to the contract are so far unperformed that the failure of either to complete performance would constitute a material breach excusing the performance of the other.}”\(^{30}\)

Section 365 specifically prohibits the assumption or assignment of certain types of executory contracts. In this range also fall contracts in which “\textit{[applicable] law excuses a party … from accepting performance or rendering performance to}” another entity, unless the other party consents. The courts have modified this definition of Professor Countryman over the years and they will usually examine the unperformed duties and obligation of the parties.\(^{31}\) Section 365(a)\(^{32}\) of the Bankruptcy code authorises the trustee to assume or reject executory contracts. According to Section 365(b) of the Bankruptcy Code a trustee may not assume the contract unless several requirements which this section imposes are fulfilled. These requirements are as follows: “\textit{[the] trustee cures, or provides adequate assurance that the trustee will promptly cure such default, compensates, or provides adequate assurance that the trustee will promptly compensate, a party}


\(^{30}\) Ibid.


\(^{32}\) See Annex I.
other than the debtor to such contract or lease, for any actual pecuniary loss to such party resulting from such default; and provides adequate assurance.”

Generally spoken the trustee has to demonstrate the ability to cure past defaults and meet future obligations under the contract. Section 365(f) of the Bankruptcy Code governs the assignment of an executory contract of an e-commerce debtor.

Under Section 365(f)(2) the trustee may assign an executory contract only under the in this section mentioned circumstances, thus offers adequate assurance to the non-debtor party in form of the benefit of its bargain.

According to this the trustee can use the let of individually identifiable data in an insolvency procedure, but the trustee has to compensate the damage the non-debtor suffers if the data is sold to a third party. The benefit of the bargain has to be paid to the e-consumer and thus there would be no benefit for the insolvent e-retailer and a breach of the privacy policy would lead to no further benefit for the company.

2.2.1.2 Solution according to Section 363

Section 363(b)(1) as solution allows the trustee to sell, lease or use the property of the bankruptcy estate. The parties in Toysmart.com and the court used Section 363 as a basis to sell the costumer list. Any such use, sale, or lease must recognise the unique qualities of intangible property. There is no section in the Bankruptcy Code, which does discuss the scope of the debtor’s interest in any

---

33 11 USCA Chapter 11 Section 365(b)(1)(A – C), see also Annex I.
34 See Annex 1.
property. Unless it can be stated that Section 541(c)(1) of the Bankruptcy Code, which establishes the property of the estate, does not increase the interest of a debtor in the property it only preserves the interest held by the debtor. The US Supreme Court stated on that matter in Butner v. United States that: "[property] interests are created and defined by state law. Unless some federal interest requires a different result, there is no reason why such interests should be analysed differently simply because an interested party is involved in a bankruptcy proceeding. Uniform treatment of property interests by both state and federal courts within a state serves to reduce uncertainty, to discourage forum shopping and to prevent a party from receiving a windfall merely by the happenstance of bankruptcy." 

According to the case of Integrated Solutions v. Service Support specialists Inc. a trustee has to take the property subject to the same restrictions that existed before the filing of the insolvency. The property of a debtor is thus limited to this extend. Hence, in the case that another party has an interest before the filing of the bankruptcy in any property of the debtor, than that interest still exists after the filing.

For example in the Toysmart.com case the e-costumers may still have had an interest in the intangible property of their individually identifiable data. Thus the FTC and Toysmart.com agreed in their settlement to sell its costumer lists only to a restricted circle of candidates. The committee of unsecured creditors opposed this settlement and claimed that the restriction placed on the proposed

35 See Annex I.
Section 363 sale of the costumer list as effectively stopping the sale before the bidding even started. The committee criticised that the costumers would have no interest that could defeat a judgement creditor or consensual lien holder. It also could not serve in any other way as a basis for a proper objection to a proposed sale under Section 363.\(^{38}\) The interest mentioned by the committee is the “interest” according to Section 363(f) of the Bankruptcy Code. This term was defined in several decisions of the federal courts. In the insolvency case of In re Leckie the sale could be ordered free of obligations to make payments to federally created employee benefit plans covering retired and orphaned coal workers.\(^{39}\) In this case coal companies had field for an insolvency procedure according to Chapter 11 and sought approval for a sale of the assets to a third party. Before the third party would agree to the sale it required that such a sale should be done “...[free] and clear of all liabilities that might arise under the coal act.”\(^{40}\) Before a decision of the court was made on the circumstance that such a sale could be executed free of all liabilities of the Coal Act the court determined that the pension plans had an “interest” within the meaning of Section 363(f). The court stated that the rights of the funds’ to collect premium payments from the debtors constitute interests in the assets “...[that] the debtors now wish to sell, or have already sold. Those rights are grounded, at least in part, in the fact that those very assets have been employed for coal mining purposes. ...Because there is therefore a relationship between (1) the funds’ rights to demand premium payments from the debtors and (2) the use to which the debtors put their assets, we find that the funds have interests in those assets

\(^{38}\) In re Toysmart LLC, No. 00-13995-CJK.


\(^{40}\) Ibid.
within the meaning of Section 363. \(^{41}\) In the Toysmart.com case it is similar. The rights of the debtor in the individually identifiable consumer data were limited to the use of this information for the purpose of personalising the online experience. The e-customers exercised their right to limit the dissemination of their individually identifiable data by disclosing this data only to one company that promised not to disclose the data to a third party without their consent. Supposed the consumers have read the privacy policy statement of Toysmart.com and agreed to provide the information on the basis of its privacy policy. Thus there is a relationship between the company’s ability to use the information and the e-consumers’ right to restrict the dissemination.

It has to be concluded that “interest” is intended to refer to obligations that are connected to, or stemming from the property, which is to be sold. According to this individually identifiable data can be sold if there is no “interest” connected to like in the Toysmart.com case. If there is another type of privacy policy – without stating that the data is not sold to third parties – there will be no interest of the e-consumer.

2.2.2 The planned Leahy-Hatch Amendment

In the line of the Toysmart.com case and other similar cases the US Senate decided to amend the Bankruptcy Code to clarify the current situation. The Senate brought the Bankruptcy Reform Bill on its way. This Bill – the so-called Leahy or Leahy-Hatch Amendment – had passed the Senate in March 2001. It contained a provision that was intended to insure the

debtor's live up to their privacy promises. The Bill is not yet law because the Congress should have voted on this Bill after the summer pause of 2001 at the 12th September 2001. Due to the September 11th attacks on New York and Washington the Bill never passed the Congress and a decision on this Bankruptcy Reform Act was postponed. The focus of the Bankruptcy Reform Bill has changed through the economic development the USA took in the last four years. After the burst of the dot-com bubble and the September 11th attacks the economy ran into a recession. In the wake of ENRON ‘s bankruptcy filings the focus of the legislators changed. A new Bankruptcy Reform Act is now in the making, but has not yet been approved by the Houses. In its section 8 are the amendments to the Bankruptcy Act, but there is going to be no amendment made to protect the privacy of e-consumers.

The draft Bill of the 107th Congress contained promising improvements and clarifications. The amendment would have been inserted into Title 11 USCA Chapter 11 § 363 of the Bankruptcy Code. The Bankruptcy Code would have clarified the situation within the field of the property law-supporting group of academics. These academics had different opinions, which kind of property individually identifiable data would have. Section 363 offers different opportunities. The data could be seen as general intangible asset, as “independent economic value” like a trade secret or copyright information. In the amendment it would have been made clear that individual identifiable data

42 Edward Janger “Muddy property: Generating and protecting information privacy norms in bankruptcy” [2003] 44 Wm. & Mary L. Rev. 1801.
44 Defiance Button Mach Co. v. C & C Metal Prods. Corp., [1985] 759F.2d 1053 decided by the 2nd Circuit, “A customer list developed by a business through substantial effort and kept in
collected from the customers by the e-retailer have to be treated as property in the form of a general intangible asset and thus are part of the bankruptcy estate.\textsuperscript{45} This provision was meant to be a clarification of the current situation; the status quo according to the Senates point of view was that lists of e-consumer data are part of the bankruptcy estate and thus property.\textsuperscript{46} If e-costumers would have had such property rights, their position for stopping the sale of their individually identifiable information in an insolvency procedure – especially when the e-retailer had promised not to disclose it in its privacy policy – would have been stronger then under current law where such property rights are missing, because there is no clarification of the status of costumer lists in the Bankruptcy Code. The trustee could have only sold the consumer list free of the e-customers interest if it would have met one of the conditions named in section 363(f) of the Bankruptcy Code.\textsuperscript{47}

It also offered the bankruptcy court to overrule the privacy policy statement of the bankrupt company. It enabled the judge to overrule “after notice and hearing”.\textsuperscript{48} This would have had the effect of a balancing of the privacy interests against the interests of the creditors in an insolvency proceeding. When an e-costumer had such property rights, their arguments for stopping the sale of their information in bankruptcy when the e-retailer has promised not to disclose the confidence may be treated as a trade secret and protected at the owner’s instance against disclosure to a competitor, provided the information it contains is not otherwise readily ascertainable. “; Avery Dennison Corp. v. Kitsonas, [2000] 118 F. Supp. 2d848. using State trade secret law in determining that the plaintiff’s customer list qualified as a trade secret.

\textsuperscript{45} S. 420, 107\textsuperscript{th} Congress § 231(a)(1)(B) to be found at http://thomas.loc.gov/cgi-bin/query/D?c107:4:./temp/~c107K1FoAR (last visited 5\textsuperscript{th} August 2004).


\textsuperscript{47} Ibid.

\textsuperscript{48} See Annex I.
data it would be stronger than under the aspect of a solely contractual situation where such rights are lacking.

Although it did not become law it is a hint how the legislator thought individually identifiable data should be treated. Following the aspect of the common law system judges can use this legislation as guideline for further bankruptcy cases. Given the new regulatory oversight of sales of costumer data in insolvency the courts will have to examine more closely the role of costumer data in each bankruptcy case.

Following the approach of the legislation individually identifiable data has to be treated as intangible property and not as a contractual obligation.

2.2.3 Conclusion from the US Bankruptcy Code point of view

The legislator tends to a property approach in the drafted Leahy-Hatch Amendment and several courts also tend to use the property approach in insolvency proceedings. The reasons for this have mainly an economic background. The property can also be used as a collateral according to Title 9 if the Uniform Commercial Code (UCC) before an insolvency procedure has been initiated and thus can be used as security for creditors. On the one side property is specially protected in an insolvency proceeding. Further can property be sold to maximise the benefit for the creditors while a purely contractual approach would bring no further benefits.

On the other side some academics disagreed with this point of view. They argue that economic interests mainly guided the courts and the legislator. They tried to
work out how individually identifiable data can be treated in an insolvency proceeding and outside such a proceeding.

2.3 Characterisation of individually identifiable information by academics

The first group of questions, which arose from the Toysmart case, was how the customer database, and therefore the individually identifiable information have to be defined. Several academics discussed different approaches in their articles. Four major groups can be found in this dispute.

Professor Jessica Litman and others argue that personal information should not be treated as property, but as a species of personal privacy and thus it shall be protected by tort law in an ex post type of treatment.49 A second group prefers to use the contractual obligations approach. This contractual view, which is outlined in an article of Miller and O’Rourke, uses two cases of the seventh circuit as a basis for this approach.50

A third group of scholars prefers to define individually identifiable information as property.51 They are attacked with the argument, if personal information is deemed property of the e-customer, information transfers that might benefit consumers will be stifled.52

---

Professor Janger has published a fourth view. It is not a clear definition of privacy and individually identifiable information as property or contractual situation. It is more an intermediatory approach. Professor Janger for example characterised the kind of property a database – and thus individually identifiable information – resembles to as muddy property or crystalline property.\footnote{Edward Janger, "Muddy property: Generating and protecting information privacy norms in bankruptcy" [2003] 44 Wm. & Mary L. Rev. 1801; Edward Janger “Privacy property, information costs, and the anticommons” [2003] 54 Hastings L. J. 899.} In the following the three different opinions shall be outlined and discussed.

2.3.1 The property approach

The academics supporting this point of view argue that according to several philosophical approaches to property personal information can be understood as property only and not as a kind of contractual obligation between two parties.\footnote{Lawrence Lessig, “Code and other laws in cyberspace” [1999] at p. 159 f., Walter Miller & Maureen O’Rourke “Bankruptcy Law v. Privacy Rights: Which holds the trump card?” [2001] 38 Hou. L. Rev. 777; Jessica Litman, “Information Privacy / Information Property” [2000] 52 Stan. L. Rev. 1283; Pamela Samuelson, “Privacy as Intellectual Property” [2000] 52 Stan. L. Rev. 1125.} They cite the labour-desert test, which was developed by John Locke in the late 17th century.\footnote{John Locke, ,,Two treatises of government“ [1690], revised edition by Peter Laslett [1960].} It seems to protect the person that collected a good and claims to have the property. Locke’ general assumption was that in the primitive state of nature there are still many unclaimed goods so that every person can collect and use these goods without infringing upon goods that others collected and use. It has to be concluded that somebody may acquire property rights in a good by
investing labour only if the good is not already the property of another individual.⁵⁶

Locke’s key assumption is that “every Man has a Property in his own Person”.⁵⁷ Locke defines a person through the individual’s personal identity. This also includes among other things the individual’s information, which is an inimitable collection of facts that makes the individual what he is. Following this theory everyone as an original property right in his individual information. Thus it has to be concluded that individual information does not exist in the state of nature, it is already owned by the individual. According to the theory made up by John Locke more the 300 years ago you can assume that personal data is property. Even more you can outline according to Locke’s theory that the property right of the collector may not prevail the property right of the individual. This can be taken from one of Lockes’ theorems. It is as follows: Somebody who picks up flowers from his neighbour’s garden, may not acquire property rights that are superior to the rights of the neighbour.⁵⁸ Following this theorem on property it can be said that data may be collected from an e-costumer legally by another party (e.g. an e-retailer) and thus the other party may acquire not the property in the whole, but the property to use the data for its purposes.

According to second theory, the Utilitarian Theory personal information can also be assumed as property. According to this theory, rights ought to be allocated so as to maximize human benefit or human satisfaction.⁵⁹ This theory has been

⁵⁷ John Locke, „Two treatises of government” [1690], revised edition by Peter Laslett [1960].
⁵⁸ John Locke, „Two treatises of government” [1690], revised edition by Peter Laslett [1960].
further developed by other academics to a theory according to which property law exists to facilitate wealth-maximizing transactions. According to the younger approaches to the Utilitarian Theory Richard A. Posner explains the theory as follows: “[whether] the law should allow a magazine to sell its subscribers list to another magazine without obtaining the subscribers consent”\(^{61}\) This focuses only on transaction cost considerations. Richard A. Posner argues that the property right in individual information should be assigned away from the individual. The reason for this is that the seller would have to obtain the costs for the approval of the subscribers. These costs would be fairly high relative to the value of the list.\(^{62}\) According to his view the cost for the disclosure of information would be very low for the subscriber. According to his arguments the purchaser of the subscriber list would not be able to “[use] it to impose substantial costs to the subscribers.”\(^{63}\)

The view of Professor Posner is vulnerable in two aspects. Firstly on the empirical grounds there are substantial costs imposed on the subscribers. Today billions of so-called spam e-mails are send to the e-consumers. It takes them a lot of working time to remove these unsolicited e-mails from their e-mail accounts. They have to bear the phone costs and the opportunity costs. If they would have worked in this time on their jobs and they would not have to erase the unsolicited mail, they could have made more money. These direct and indirect costs are

---


\(^{61}\) Ibid.

\(^{62}\) Ibid.

imposed on the customers every day.\textsuperscript{64} Further costs through telemarketing and paper based junk mail are also factors to be taken into account.

Secondly on the theoretical grounds this view is problematic. The property regime promulgated by Posner and others creates externalities.\textsuperscript{65} Externalities mean in this context that social costs associated with the collection and trade of individual information are not fully borne by primary and secondary collectors. Instead these costs are borne by the consumer himself who gave away some of his individual information, and another part is borne by the general public. This fact also weakens the arguments of the promulgators of the Utilitarian Theory on property. But even with these weaknesses the individual information is property.

Another group puts another emphasis on the theory of Hegel and do not concentrate on the economic efficiency as much as Posner and others do.\textsuperscript{66} The underlying premise of the so called Personality Theory of Property is that to achieve proper self-development – to be an individual – someone needs some control over resources of the external environment. In the eyes of these academics one can distinguish between two different types of property. Firstly there exists a property bound up with a person. Secondly there is a kind of property that is held purely instrumentally – these academics call it personal property and fungible property.\textsuperscript{67}

The first type of property is bound to its person and cannot be compensated in cash. The only possible compensation is the return of the lost object. The second

\textsuperscript{64} E.g. the author of this dissertation receives 50 to 75 unsolicited e-mails every day. Cleaning up the e-mail account and downloading the spam-mail takes approximately 10 minutes every day.


\textsuperscript{66} See above FN. 29.

type can be compensated in cash because the proprietor of the item has no personal affection but only instrumental reasons. According to this distinction both types of property shall be treated in different ways. In the following Professor Radin makes a distinction between individual information held by the person himself and the collector that has collected the data. According to all these theories discussed they have one thing in common, they all assume that individual information is property and shall be treated as such in a bankruptcy proceeding.

2.3.2 The ex ante contractual approach

The academics promulgating this version assume that the transfer of data is solely a contractual obligation. They base their arguments on two judgements of the 7th Circuit made in the years 1996 and 1997. In these cases a costumer bought a product that was packed in a box and in these boxes were further terms and conditions dealing with the use of the product. In the ProCD case it was mentioned on the box, that this box contains further terms and conditions. The court stated that: “ProCD proposed a contract that the buyer accepted by using the software after having an opportunity to read the license at leisure.” Following this argument the terms and conditions in the box bound the costumer who did not return the bought product and by doing this rejected the proposed

---

68 Ibid; Radin gives an example of a husband loosing his wedding ring and a jeweller loosing a wedding ring.
69 Ibid at FN. 37.
terms and conditions. The customers in the second case ordered a product by phone. The package delivered to the customer contained detailed terms and conditions. In this case the court held that the buyer and the seller concluded a contract including the terms and conditions. The consumer could only abstain from the contract when he returned the bought computer within the set time limit set in the contract. These cases of so called “shrink-wrap” licenses were used by several other courts in other decisions on the sale of software and computers. The reason for this was that the Court in ProCD held that its reasoning is not only limited to this case but can be used for all other cases involving software and other high-tech goods or services.

Transposing the rationale of these cases on the Toysmart.com case would lead to the conclusion that the privacy policy statement of this company would have been a part of a contractual relation between the e-costumer and the insolvent company. Thus the let of individually identifiable data would become a solely contractual relation between the two parties. The e-costumers would have agreed to the policy by ordering products from the now insolvent company. In line with the above-mentioned judgements in the cases ProCD and Hill, this act of ordering articles with the chance to know the content of the privacy policy statement is enough to incorporate these terms into the contract. When contractual terms with disadvantageous content can become part of a contract advantageous have to be moreover than the aforementioned become part of the

75 Ibid.
contract. The contract preferring academics find it even more convincing that the privacy policy of Toysmart.com became a part of the contract because the e-consumer had the opportunity to read and accept the terms prior to the purchase.79

2.3.3 The ex post viewed tort approach

Another approach denies that personal information is property. These academics argue that information seems to be a kind of tort law matter. With this point of view they defer from the group preferring a property approach. This group uses a contractual view of the matter, while they assume that the let of individually identifiable data lies within the field of privacy and thus privacy is a solely contractual obligation, which is inter alia protected by tort law. The demand that privacy should be treated as distinct tort for which a remedy should be made available was proposed for the first time in 1890 in an Article written by Samuel Warren and Louis Brandeis.80

This group prefers the ex post view – how to deal with the matter after privacy rights are probably violated. Two academics developed in the year 2000 their approach to personal information as obligation governed by tort rules. In two articles Professor Jessica Litman and Professor Pamela Samuelson clarified their idea of personal information as part of personal privacy governed by tort.81 According to them individual information has to be protected by tort law.

79 Ibid.
Especially the breach of confidence would fill the gap how individual information can be protected. “[A] tort law breach of trust approach does have significant advantages over a privacy-as-property model. It avoids the trap of alienability and the perverse incentives that market in alienable personal data would create. Because it forgoes the privacy-rights-management market entirely, it is less likely to legitimise wholesale commercial exploitation of personal information.” Following this approach it would permit courts to discriminate between consensual and invasive disclosure ex post and could make judgements to compensate a violation of privacy. It has to be pointed out that in the same moment a tort-based approach would be at least as easily achieved as a property-rights system. This is based on the fact that common law tort jurisprudence is more intuitive than the codified tort system in continental European jurisdictions is. Litman also argues that a breach of trust still is the essence of something that embarrasses people about the commercial use of their individual information, thus it would make it easier to persuade courts to endorse the theory. Also would lead this approach to a federal statutory protection of individual information. Tort litigation would be a possible route to enact federal laws on data protection.

2.3.4 The combined approach

In the early seventies Professor Calabresi and Mr. Melamed wrote an article dealing with the property rules, liability rules and inalienability. This approach

---

83 Ibid.
was the first approach on this field of law combining the advantages of property law and tort law to a new system. It broke up with the strict segregation of these two systems.\(^8^4\)

The first aspect the authors are dealing with is the aspect of “entitlement.”\(^8^5\) In the case that a state is confronted with two conflicting parties, it has to decide which side to favour. An “entitlement” is protected by a rule of property. According to the article of Calabresi and Melamed it is protected by the property rule “… that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller.”\(^8^6\) The special form of the entitlement gives rise to the minimum amount of state intervention. When the original entitlement is decided upon the state does not evaluate it. It lets both sides of the parties evaluate the entitlement and gives the selling party a veto if the buyer does not offer enough. To whom an entitlement is given is a collective decision on property rules, but not to value it.\(^8^7\) Thus private property can be seen as an entitlement, which is protected by a property rule. But the theory of Melamed and Calabresi does not stop at this point they developed the idea further and concluded that an entitlement can also be inalienable. According to their theory the state has only a right to intervene to determine the compensation that must be paid in the case, that the entitlement is taken or destroyed without the consent of its owner. Also the state can be allowed to forbid the sale under some or all

---


\(^8^5\) Ibid.

\(^8^6\) Ibid.

\(^8^7\) Ibid.
circumstances. \(^8\) According to Melamed and Calabresi rules of inalienability “not only protect the entitlement, they may also be viewed as limiting or regulating the grant of entitlement itself.” \(^9\) Another mechanism to protect the entitlement is the liability rule. It is an external and objective standard of value. This is used to facilitate the transfer of entitlement from the holder to the buyer.

Professor Janger takes up the arguments of the Melamed and Calabresi article and tries to open the thesis of the authors up for the new development in bankruptcy and privacy law. He states in a series of articles that with his type of definition the problem of e-consumer databases in a bankruptcy can be solved. His approach highlights two problems. He categorises it as the “right” problem and makes a distinction between muddy and crystalline rights. Further he discusses the problems of the remedy as issues of property versus liability. \(^0\) As a last aspect he discusses the problem of the “judgement proof”, which was developed by economists in the mid 1980’s. \(^1\) The “judgement proof” theorem says that a liability that exceeds the assets of an injurer is going to be treated by him as a penalty as an effective financial penalty only equal to his assets. \(^2\)

Janger puts all these above-mentioned parts together to one system. This system is called system of “muddy property rights.” The main interest of the author is to find a balance of power between the financial interests of the creditors on the one side and the privacy interests of the customers on the other side. Professor Janger defines “muddy” rules as rules serving two different functions. The first is to

---

\(^8\) E.g. when the seller is a minor.

\(^9\) Guido Calabresi and A. Douglas Melamed, op cit. at FN. 84.

\(^0\) Edward Janger, “Muddy property: Generating and protecting information privacy norms in bankruptcy” [2003] 44 Wm. & Mary L. Rev. 1801.


deter troubling transactions. The second purpose is to force contracting parties, ex ante, to recognise that they might have to justify their contractual terms ex post. In the context of privacy they also should serve a third purpose. “Muddy” rules would force individual information into the legal system about norm-related behaviour. In turn this would allow judges to enforce and articulate privacy norms through the incremental development of common law rules. A so-called “muddier” standard would leave the right subject to challenge by a competing claimant. Following the theory of Professor Janger so-called “crystalline” rules situate decision-making and norm-generating authority either the legislature or the market. Thus muddy rules would lead to judge-made decisions and legal norms articulated by courts.

In the first line Professor Janger promulges a property-based entitlement that establishes the scope of data privacy in bankruptcy. And this definition of property is based on the judge made decisions of the common law system. In a second step he assumes that the entitlement shall be protected by liability rules to safeguard the privacy policy of the website. Thus if the e-retailer breaches the privacy policy in an insolvency proceeding a liability in the form of civil damages would come up and protect the interests of the e-consumer.

2.3.5 Solution of the problem of defining data in an bankruptcy

To find a solution to the problem it has to be pointed out what kind of advantages and disadvantages each of these theories have. Seen from the

94 Ibid.
95 Ibid.
position of the tort preferring academics pursuing a tort law strategy for privacy protection would be preferable instead of the solely property rules based approach. The reason they give for this is on one side the effectiveness of tort and that it would be comparatively benign than the property law approach.\footnote{Pamela Samuelson, “Privacy as Intellectual Property” [2000] 52 Stan. L. Rev. 1125; Jessica Litman, “Information Privacy/ Information Property” [2000] 52 Stan. L. Rev. 1283.}

Following the argument of the ex post tort law approach the property approach would be too slow to be enforced and it would bring a lesser benefit to the e-consumer. While the process at the court continues the company still would be able to collect more data and could put it together to more detailed user-profiles. Another argument is that property interests are generally alienable. As such if a particular interest is not alienable, this outcome must be due to some rule against the alienability of such an interest. The policy of the law and the courts has been generally in favour of a high degree of alienability of property interests in an insolvency procedure. This standpoint stems from the belief that the social interest is promoted by the greater utilisation of the subject matter of property, caused by the freedom of alienation of interests in it.

From the point of view of the tort promoting academics the reason for property is its alienability and thus that the purpose of property laws is to prescribe the conditions for its transfer. According this opinion property law gives the owners a control mechanism and also the ability to sell and license the item. Control is a “right to exclude” others from property. It is related to different sorts of control conferred by different branches of the law. It is not necessary to treat an interest in data as property in order to protect it from invasion of third parties. Therefore stands usually the domain of tort law. For this there can be given some examples
of different branches of tort law protecting different aspects. The law of battery protects the integrity of the body, even though the body is no longer seen as property in the US jurisdiction. The law of integrity protects somebody’s reputation, though the reputation is not property. The same applies for torts concerning anti-discrimination; the interest in freedom from invidious discrimination is not seen as property. Alienability is not deemed to be the important point of individually identifiable information, this information is more related to the integrity or discriminatory issues above mentioned and should be protected in the same way because it is very close related to it. This is also intended to bring an end to the pressing claims of so called data-miners that already claim to have proprietary interests in the information they have already compiled.

The approach of the group preferring the contractual approach argue, that in the case that damages would not compensate the affected person for the loss, a court may grant an injunction or specific performance. This transposed on a case like Toysmart.com could mean that the court may enjoin the bankrupt company from releasing the database to the buyer. It would be also possible that the court may define the group of companies to which the data can be sold. The e-costumer has to proof that he suffered an irreparable harm, if the individually identifiable data would be sold. Miller and O’Rourke proposed that an e-costumer could argue that the harmful event is the broken promise of the company’s privacy policy. This is the weakness of the contractual approach. If the privacy policy is


different from the policy of Toysmart.com, like the new policy of Amazon.com the e-costumer would not have a claim for a harmful event and thus his claim would not have a legal basis. Further it is difficult to calculate the damages. A practical enforcement of this approach is merely impossible. Also has to be mentioned that contractual obligations can be discharged in an insolvency while property rights are not discharged.\footnote{Dewsnup v. Timm, [1992] 502 U.S. 410.}

One aspect, which is brought forward by the academics that prefer to use the property-based approach, is that privacy law torts are limited. Under normal circumstances tort law only protects personal data from disclosure when it conveys embarrassing personal information or is used for defamation and discrimination. But gathering data is not actionable at all, unless the gathering behaviour, the compiling and exploitation of the data is itself highly intrusive. Here the e-consumer does not want that the data be transferred in an auction during an insolvency procedure to a third party without their prior consent. The missing consent cannot be seen as highly intrusive.

The approach of Professor Janger tries to combine the above-mentioned issues to a new kind of view, how the individually identifiable data should be characterised.\footnote{Edward J. Janger, "Muddy property: Generating and protecting information privacy norms in bankruptcy" [2003] 4 Wm. & Mary L. Rev. 1801; Edward J. Janger, “Crystals and Mud in Bankruptcy Law: Judicial Competence and Statutory Design” [2001] 43 Ariz. L. Rev. 559.} The legal treatment of privacy policies in bankruptcy currently turns on whether such policies are viewed as creating contract rights or property rights. Neither characterisation fits well, and any attempt to shoehorn information privacy into either category has significant costs (risks). Contractual obligations are subject to discharge in bankruptcy, and any consumer
expectations of privacy (contractual or otherwise) are likely to be defeated. Because without being “property,” information privacy norms will go entirely unenforced.

By contrast, if personal information is deemed property of the website costumer, information transfers that might benefit costumers will be stifled. When the privacy policy is solely treated as contractual obligation, the debtor will be free to breach the contract in an insolvency. The reason for this is the position of an e-consumer as a claimant. His damage claim will be treated as a pre-petition claim. Every damage paid, if so, will be paid at a significant discount. When the individual information is treated as property, the interest in property must be given protection.

In the end one can say that the academic approach of Professor Janger and others is preferable. The combination of property rules and liability rules give the most effective protection to the e-consumer. The data of the consumer is protected in a bankruptcy and safer than in any other regime outlined. It is convincing that an insolvent e-retailer has the liability to pay damages in the case that the property law is not obeyed. This opens up the opportunity to protect the privacy interests in the most effective way.

2.4 The Privacy Law

Now that it is worked out how individually identifiable data can be protected under the bankruptcy law it has to be analysed in which way the privacy law

---

102 See Annex I, 11 USCA Chapter 11 section 365(g).
103 See Annex I, 11 USCA Chapter 11 section 361.
within the United States protects the interests of e-consumers when an e-retailer has filed for an insolvency. The United States derives privacy as a principle from different amendments of the Constitution. There are often mentioned the first, third, fourth, fifth and fourteenth amendment that shall contain privacy rights as “rights to be let alone.”\textsuperscript{104} Also there is no right to informational privacy acknowledged by the US Constitution or mentioned in a decision of the Supreme Court.\textsuperscript{105}

Generally data protection law is not a federal law issue. At the moment each State has its own privacy law model and there are only some issues ruled in federal laws. Federal law shall only rule on certain distinct fields of data protection and privacy rights. The general idea of the US legal system is the idea of self-regulation. Thus privacy policies and codes of conduct are more important. For example the Gramm-Leach-Bliley Act rules only on aspects of privacy in relation with financial services while the Children Online Privacy Protection Act (COPPA) only protects the interests of minors. Further there is the FTC Act, which generally deals with consumer protection. Based on these three acts it shall be outlined how privacy law protects e-consumers nowadays and how it could protect them in the future.

2.4.1 Gramm-Leach-Bliley Act of 1999

In 1999 the Gramm-Leach-Bliley Act (GLB Act) sought to provide new rules in the field of financial privacy law. It should have limited the possible negative

\textsuperscript{104} Susan E. Gindin, “Lost and Found in Cyberspace” \url{http://www.info-law.com/lost.html} (last visited at the 7\textsuperscript{th} September 2004).

\textsuperscript{105} Ibid.
results of data processing by the financial market.\textsuperscript{106} This act contains privacy provisions that deal with four different issues of privacy law. In the first place it demands that financial entities under its regulation have to provide annual privacy notices. These notices shall inform the e-costumers of their privacy practices. Further it requires this group of financial entities to permit their customers to prevent them to share the individually identifiable data with non-affiliated companies. To be more precise the GLB Act has ruled this on an “opt-out” requirement.\textsuperscript{107} This means that any e-costumer who does not wish to have his individually identifiable data given to a non-affiliated company has to inform the company not to do. The third issue deals with the development of data security policies. Last but not least the GLB Act provides enforcement rights. It is not assigned to individuals, but to federal agencies like the Federal Trade Commission.

2.4.2 COPPA

There is another federal approach to protect a group of e-consumers by a special legislation. Especially this law made the FTC sue against the sale of the individually identifiable data in the Toysmart.com case. The Children Online Privacy Protection Act of 1998\textsuperscript{108} was aimed to protect minors under the age of 13 years. The e-retailer has to display its privacy policy containing what kind of data is collected and what kind of disclosure practices they have. Then the


\textsuperscript{107} Ibid.

\textsuperscript{108} 15 USCA §§ 6501 – 6506.
parents of the underage have to give their consent to the privacy policy. If this consent was given than it was permitted to store and compile the data according to the terms and conditions of the privacy policy. According to this Act there is no restriction in the sale of data to third parties when the parents agreed to it by ticking a box next to a text field that may display the following: “I agree with the privacy policy of this company.” When the consent is given there is no further restriction for the e-retailer, hence the data of the underage children can be sold in- and outside of an insolvency procedure. According to 15 USCA § 6502(b)(1)(A)(ii) this consent has to be “verifiable.” A further clarification is not given by the code what verifiable means.

It applies to operators of websites and online services that are specifically directed at children under the age of 13. Further it is also directed to website operators of all other websites that have actual knowledge that they are collecting data of underage children.

The FTC is authorised to control the online retailers to enforce the Act. As in the GLB Act there is no right assigned to individuals to enforce the Act, but to a federal agency. Parents have the right to withdraw the permission to collect data at any point of time and can request to provide a description of the individually identifiable data collected.

2.4.3 Conclusion Data Protection Law

Thus federal Acts can be seen as a bottom line of privacy protection in the sector of financial privacy law and minor protection law. At the moment there is no general privacy law at the federal level, that protects other privacy issues of e-
costumers but the afore mentioned. In general the federal government prefers to grant the e-business more space for self-regulation than for governmental restriction. Thus the federal government has left it to the e-retailer if it wants to sign a contract with another privacy rights guarding organisation like TRUSTe, which shall secure certain privacy standards. Only if the privacy policy of an e-retailer like Toysmart.com was so clear that it would not sell its database to a third party at any point of time it was possible to protect the e-consumers. The FTC would see a sale as deceptive business practice and would interfere. To circumvent this Amazon.com changed its privacy policy after the Toysmart.com case. The company informed all 23 Million users that the consumer database is going to be sold as assets in the unlikely event of insolvency.  

The consumer has no special right stemming from the federal privacy laws to have his data removed from the database before the data is sold. Only in the case of the GLB Act there is an “opt-out” rule that a consumer can object the sale. This assumes that an e-costumer has to object actively to have his data excluded from the sale. This “opt-out” requirement can also be found in the “Can-Spam” Act of 2003, which is in force since the 1st January of 2004. This act contains in its Section 5(a)(4) the “opt-out” principle as general rule. E-mails for marketing purposes have to contain the information that the e-consumer has the right to opt-out. A sale of individually identifiable data of e-costumers that opted out is also forbidden.

110 Title 18 USCA Chapter 46.
111 Title 18 USCA Chapter 46 Section 5(a)(3).
112 Title 18 USCA Chapter 46 Section 3(17).
Another option is not used in the U.S. federal law, which is the “opt-in” requirement. Thus the consumer does not have to object the sale of his data, he has to agree to the sale. The “opt-in” requirement is criticised strongly in the United States. An “opt-in” requirement would create strong disincentives for companies and thus they would forbear from desirable information transactions. The reason for this would be the fear that the costs approaching the e-consumer to request a permission me be higher then the extractable value of the underlying individually identifiable data.113

2.5 Conclusion from the United States point of view

In the United States there are still no special laws made for the sale of data in an insolvency procedure. Even though this system had to deal with the most insolvencies in the recent years. The legislator tried to change the situation. A promising approach was made in 2001 when the Bankruptcy Reform Act was on its way. A classification would have been made, and costumer data would have been qualified as intangible property. Now that the Bankruptcy Reform Act is stopped and the Leahy-Hatch Amendment is not part of the US legal system. Hence it is still not well defined how costumer data has to be treated.

Also the Leahy-Hatch Amendment would not have solved another problem of the sale of costumer data. It did not qualify how the costumer’s consent to the sale of their individually identifiable data has to be declared. It even gave the judges the opportunity to agree to a sale under certain circumstances without the consumers’ consent. It is still not clear if a consent of the consumer is required or

not and if how this consent has to be made. According to the GLB Act the US federal law prefers to use the “opt-out” system as viable. And is using this only for the financial services sector which usually requires a higher degree of protection than any other field of business.

In In re Toysmart the FTC and the debtor used the “opt-in” system in the settlement. This “opt-in” system was based on the idea to protect the underage children that gave data to the insolvent online retailer. On the same basis the fact has to be seen that the individually identifiable data should only be sold to a qualified buyer that operates in the same part of business and offers an equal privacy policy. This leads to a further problem, the aspect of the privacy policy statement of the e-retailer. When it is stated in the policy that the data is going to be sold in an insolvency there is no further consent needed from the consumers.

All these unsolved points lead to an approach to a solution how individually identifiable might be treated in an insolvency. Thus a catalogues of aspects shall be checked before these assets are sold to a third party. Before a sale of e-consumer data is attempted in an insolvency situation, the insolvent company shall assess whether the data was legally compiled and stored.\textsuperscript{114} Especially it shall be checked for possibly violating the COPPA or GLB Act. Otherwise the FTC or State attorneys may interfere the sale. Though the purchase may not be objected it is possible that the new owner of the data can become an object of future regulatory action.

Having determined whether the company’s individually identifiable data compilation and the use of policies comply with the technical requirements of the privacy protecting statues requires the analyses of the privacy policy in the light of the applicable provisions. Further it has to be determined if the intended sale of data would constitute an unfair or deceptive business practice violating the FTC Act which is by far more difficult.

In the Toysmart.com case the FTC pointed out that the privacy policy promised the customer not to sell any of the individually identifiable data to a third party, every sale of the data would be a deceptive business practice. This position of the FTC cannot be held. If a privacy policy would be drafted in a different way, like amazon.com and ebay.com did a sale would be according to the FTC arguments be not a deceptive business practice. Here further points should be added to the catalogues of aspects, which should be checked before a sale of data. A sale should depend on the identity of the buyer, is it a mass mail enterprise or not. Does the buyer have the same privacy policies concerning the use of its costumer data?

Then it should be considered how the costumers themselves could approve a sale of costumer data. Generally there are two possible systems. In the Toysmart.com case the FTC indicated that it is acceptable when the costumer is informed of the sale and affirmatively agrees to the sale, the so-called “opt-in”. This system has not only the advantage that the costumer has to agree actively e.g. by sending an e-mail to the selling company it also raises the value of each sold set of data. The consumer made clear that he is interested in the sale and there is a higher possibility that this consumer will use the website of the new owner of the data.
more frequently. This also gives the e-retailer the opportunity to erase data of only nominal e-customers that are no more interested in its homepage. The mentioned factor of the costs is marginal. A mass e-mail to all the e-mail addresses in the customer database is very cheap and the programme to relate a replied answer to a specific set of data is also not very expensive. This system has the further advantage that it is going to reduce the risk of regulatory action by customers that disagree with a sale of their data.

These points will lead to a balance of interests. Other points like the ombudsman mentioned in the Bankruptcy Reform Act of 2001, which did not enter into power, are further aspects to consider. An ombudsman could also work together with a trustee to structure guidelines for the sale of customer data.\textsuperscript{115} This would lead to the result that a trustee does not want to propose such a sale and has to find out, that the ombudsman does not support the terms of the sale the trustee has appointed. On the other side the trustee will not agree to too strict terms the ombudsman may set to the sell and might over protect the privacy issue. By providing a certain degree of consolation with sale terms, an ombudsman can help the trustee to maximise the financial revenue a sale of customer data may bring. This mechanism would be very helpful in the field where a privacy policy may strictly prohibit the sale of such data.\textsuperscript{116}

In the case that a buyer does not want to acquire the data solely, but tries to buy the whole stock of customers, there are several methods to do such a transfer and thus circumvent the above-mentioned mechanisms to control the transfer of individually identifiable data. Agin gives some examples to circumvent the


\textsuperscript{116} Ibid.
control of a data transfer in one of his articles. In this example the selling company might agree to forward the buying company’s marketing materials to the customer list for a certain amount of money, rather than transfer the customer list. A second possibility to do so is for the insolvent company to refer customers to the third party. The third party pays a fee either for every customer referred, or for every customer that actually purchases goods or services from the third party.

In the end there is no proper solution to be found in the United States on the grounds of the existing legislation and jurisdiction. In the future the academics and the practitioners have to find a solution to strike a balance between the interests of the e-consumers and the interests of the creditors of an insolvent company.

3. Chapter 3 - Approach of the EU legislation and further development

After working out the way how the United States of America have dealt with the issue of the sale of individually identifiable data of e-consumers in an insolvency proceeding it shall be worked out how the European Union and there especially the Federal Republic of Germany has solved the problem.

Firstly there has to be given a short overview of the EU legislation on privacy law and data protection law the EU has made within the last decade. The EU has brought up several Directives to protect the privacy of the consumers. The core is formed by the Data Protection Directive 95/46/EC and the Directive

---

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.\textsuperscript{118}

The EU privacy legislation can be seen as a two-step model. The first step is the collecting of the data. Article 13(1) of the Directive 2002/58/EC governs the compiling of the data. In this provision is ruled that an e-customer has to “give his prior consent to the compilation of his data.” This indicates a general “opt-in” rule. However it is not clearly defined how this consent has to happen. According to Recital 17 and Article 2(f) of the Directive 2002/58/EC refer to the Data Protection Directive95/46/EC. This Directive defines the “consent” of a data subject as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data related to him being processed”.\textsuperscript{119} Consent in the context of the Directive 95/46 is not specific to communications for direct marketing purposes.\textsuperscript{120} There are several ways by which a consensus may be found in accordance with the EU law. Momentarily there is no specific provision found how the consent has to be given by the e-consumer. According to Recital 17 of the Directive 2002/58/EC “… Consent may be given by any appropriate method enabling a freely given specific and

\textsuperscript{118} Directive 2002/58/EC of the European Parliament and the Council of 12\textsuperscript{th} July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication) if further mentioned in the essay it will be cited as Directive 02/58.

\textsuperscript{119} Art 2(h) of the Directive 1995/46//EC of the European Parliament and of the Council of 24\textsuperscript{th} October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data – if further mentioned in the essay it will be cited as Directive 95/46.

informed indication of the user’s wishes, including by ticking a box when visiting an Internet website.”

According to this a Working Paper of the Art. 29 Working Group stated that a list which has not been established in accordance with the prior consent requirement may in principle not be used any more under the “opt-in” regime, at least until they have been adjusted to the new requirement. The sale of such an incompatible list to a third party is also illegal. An e-retailer wishing to buy such a list of individually identifiable data should be cautious that such a list is in accordance with these requirements. Especially the e-retailer has to proof that prior consent was given in accordance with those requirements. The only exception that can be made is the data, which was collected from existing costumers. This working paper gives the space for the conclusion that a sale of e-costumer data is generally legal, if the aforementioned requirements of its collection are met. Especially this first step demonstrates that the EU does not prefer the use of self-restriction and corporate guidelines like a code of conduct – something also called as “soft law” – as a system of privacy law, but a system of “hard” law made by the government.

The second step of this model is the duty to inform the e-costumer about the sale of his individually identifiable data. According to Article 14(b) of the Directive

---

121 Recital 17 of the Directive 02/58.
95/46 the party that wishes to sell the data to a third party for marketing purposes has to inform the e-customer about the sale. After this the customer has a right to object the sale of the data. This constitutes an “opt-out” regime for the sale of data.

This general scheme is ruling on the sale of data in the usual course of business. Now the question comes up if this scheme is transferable to the sale of customer data in an insolvency. In this case the intentions why the data is sold to a third party changes, a trustee wants to satisfy the interests of the creditors. But for the e-consumer the interest does not change and there is no change in the quality of data, which is sold. So this gap between the interests, the speed of the liquidation and the privacy interest of the e-consumer, has to be balanced once more. The two step system of “opt-in” for the collection of the individually identifiable information and then following by the “opt-out” in the case of a sale of the data corresponds to both of the abovementioned interests. According to both Directives there is no certain formal requirement for the information about the sale given. Thus an e-mail would be enough to meet this requirement. This is an inexpensive and fast way, which does not affect the speed of the liquidation. Also it is protecting the interest of the costumer, because he receives the information in a proper way and has no further expenses than the usual expenses he has for the connection to the Internet. The consumer can object the sale of his data in the same fast way, by sending an e-mail.

Secondly it has to be pointed out, that there are no insolvency provisions given by the European Union that may rule on the sale of individually identifiable data.

---

125 Art. 14(b) of the Directive 95/46/EC.
in an insolvency procedure. Until today the EU was reluctant to develop a Regulation or Directive on issues concerning bankruptcy. The only Regulation dealing with this aspect was a Regulation to harmonise the cross-border insolvency procedure within the EU.\textsuperscript{126} Like the so-called Brussels Regulation\textsuperscript{127} this Insolvency Regulation gives only rules for the enforcement and recognition of judgements. Thus national law governs the characterisation of individually identifiable data.

4. Chapter 4 - National laws on e-consumer protection in an insolvency in the EU

The German law was restructured in the last five years to meet the requirements of the modern technologies. Thus the “Bürgerliche Gesetzbuch” the German civil code was changed in the field of the law of obligations.\textsuperscript{128} This is the fundamental change in the German law, which gave the e-commerce a legal basis in the German legal-system and thus is the starting point for the collection of e-consumer data. The German Insolvency Code was also modified.\textsuperscript{129} It contains now rules of reorganisation like Chapter 11 of the US Bankruptcy code which was the blueprint for the this part of the new Insolvency Code §§ 217 – 269 of the Insolvency Code.\textsuperscript{130} This new code does not give any references to the


\textsuperscript{127} Council Regulation No. 44/2001 of 22\textsuperscript{nd} December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.

\textsuperscript{128} Civil Code of the 18\textsuperscript{th} August 1896, complete revision of the law of obligations of the 1\textsuperscript{st} January 2002 to implement the Directive 2000/31/EC on e-commerce, last revision of the 15\textsuperscript{th} July 2002.

\textsuperscript{129} Insolvency Code of the 1\textsuperscript{st} January 1999, last revision at the 5\textsuperscript{th} April 2004.

sale of assets in the form of an e-costumer database explicitly. Thus it has to be analysed if the provisions on the insolvency proceeding contain rules, which are applicable on this specific problem.

4.1 Characterisation of individually identifiable data in Germany - alienability

The problem discussed above dealing with the issue how individually identifiable data has to be treated in the US legal system has not been discussed in such a way in Germany. The right of “informational self-determination” is seen as one of the fundamental rights granted by the German “Grundgesetz” – the Basic Constitutional Law. In one of its most important decisions the Federal Constitutional Court\textsuperscript{131} ruled that the right for privacy is not explicitly mentioned in the Basic Constitutional Law but can be derived from the Articles 1 and 2 of the Law.\textsuperscript{132} In the first line it was only ruled on the relation between the state and the citizens later also in the relation between the citizens. The FCC ruled in its decision that “every individual shall have the capacity to determine the relinquishment and use of his personal data.”\textsuperscript{133} This means that individually identifiable data is a kind of property, which is in generally alienable except for some data that is explicitly mentioned in the codes on data protection and privacy like the Federal Code on data protection. The property a data processing e-retailer receives is compared with the property rights a tenant gets when he

\textsuperscript{131} Further abbreviated with FCC.

\textsuperscript{132} Decision of the Federal Constitutional Court of the 15\textsuperscript{th} December 1983, BVerfGE 65, p. 1 so called “Volkszähungsurteil – judgement on the population census”.

\textsuperscript{133} Decision of the Federal Constitutional Court of the 15\textsuperscript{th} December 1983, BVerfGE 65, p. 1 at p. 46.
rents a flat from a landlord. The e-retailer has the right to compile the data and use it for his business purposes. He is not allowed to sell the data without the consent of the individual, like a tenant is not allowed to rent the flat to a third person without the consent of the landlord according to German law. According to German law a tenant gets a restrained property of the flat, which is limited to some extend. This can also be concluded from the judgement of the FCC in regard to the use of individually identifiable data. Thus individually identifiable data is alienable property, which can be given to third parties only with the consent of the individual. It also can be found in § 4(1) of the Federal Data Protection Code and in Article 13(1) of the EU Directive 2002/58 on privacy and electronic communication. § 4(1) of the Federal Data Protection Code states that: “the collecting, processing and use of personal data is only permitted, as far as this code or another provision this allows or orders or the affected person gives his consent.” Individually identifiable data is seen as property with certain limitations on its alienability.

4.2 German Bankruptcy Code

At first a short introduction into the German Insolvency Code has to be given. Like the US Bankruptcy Code the German Insolvency Code triggers a stay of proceedings according to § 23 of the Insolvency Code, as soon as a debtor files for an insolvency and the insolvency procedure is started. Then a receiver is appointed this is ruled in § 56 of the German Insolvency Code. This receiver has

---

similar rights like the trustee in the Bankruptcy Code. The receiver takes all
assets in possession and on trust.\textsuperscript{136} This person has to give a statement of assets
and liabilities in which all assets and liabilities have to be disclosed and assessed
according to § 153 of the Insolvency Code.\textsuperscript{137} In line with § 35 of the Insolvency
Code all assets also intangible assets like trade secrets are part of the insolvency
estate. Transposed to the problems outlined above the German system has no
problems to categorise the database containing individually identifiable costumer
data as intangible property and thus as an asset under the German Insolvency
Code. There is no problem to categorise it as property and not as contractual
obligation like the US system does. The leave of personal information is a
contractual situation governed by the privacy policy of the insolvent company. In
§ 103 of the Insolvency Code\textsuperscript{138} is ruled that the receiver has the choice to fulfil
a contract that is yet not performed, or discharge. This approach is in this point
like the Countryman definition for the US Bankruptcy Code. But this provision
goes beyond the approach of the US academic it sets up the requirement that
these types of contract have to be reciprocal that the performance of each party is
directly related to the performance of the other party. The Greek term of a
"synallagma" is used for this special contractual situation.\textsuperscript{139} The promise not to
sell data to third parties can thus not be seen as such a contractual situation
because there is no consideration, no \textit{quid pro quo} in the sense of German law.
This clause is not the primary object of the leave of data it is only an
accompanying clause, a secondary obligation. Thus the contractual basis

\textsuperscript{136} § 148 of the Insolvency Code of the 1\textsuperscript{st} January 1999, last revision at the 5\textsuperscript{th} April 2004.
\textsuperscript{137} See Annex I.
\textsuperscript{138} See Annex I.
\textsuperscript{139} E.g. giving money getting a loaf of bread.
discharged with the filing of an insolvency procedure and thus the database can be sold according to the German Insolvency Code. There is no consensus needed from the view of this code. Thus it can be said, that a sale of individually identifiable costumer data is generally allowed according to the Insolvency Code.

4.3 Germany’s approach from the privacy law point of view

On the other side the receiver has also to obey the codes not dealing with an insolvency procedure. There are at least three different codes dealing with the issue of privacy and the compilation of data in the Internet. There is the Federal Data Protection Code “Bundesdatenschutzgesetz”\textsuperscript{140} in the first place as general code for data protection, further there is the Tele-Services Code “Teledienstegesetz”\textsuperscript{141} and the Federal Treaty on Media Services “Mediendienste Staatsvertrag.”\textsuperscript{142} Both laws rule on some parts of the collection of data in the Internet. The first mentioned is a federal law the second is a treaty of all states “Länder” without the participation of the federal government. These laws have to be seen as lex specialis, though these codes provide no solution for the problem of the sale of individually identifiable data the lex generalis, the Federal Data Protection Code has to be considered.

\textsuperscript{140} Federal Data Protection Code – “Bundesdatenschutzgesetz” of the 14\textsuperscript{th} January 2003.
\textsuperscript{141} Tele-Services Code “Teledienstegesetz (TDG)” of the 14\textsuperscript{th} December 2001, formerly known as Informations- und Kommunikationsdienstegesetz (IuKDG).
\textsuperscript{142} Federal Treaty on Media Services “Mediendienste Staatsvertrag” of the 27\textsuperscript{th} July 2001, last amended at the 20\textsuperscript{th} of February 2003.
4.3.1 German lex generalis on privacy

The most important provisions are now going to be outlined and it shall be worked out how these provisions may protect the data of an e-costumer in an insolvency procedure in Germany. The possibility of the sale or lease of data from the e-costumer to the e-retailer has already been outlined above. According to § 4 (1) of the Federal Data Protection Code it is allowed to compile and use the data with the consent of the costumer. This general rule is modified by § 28 of the same code if data is going to be used for economic and other non-administrational reasons. A receiver in an insolvency would have to regard especially the following rules.

4.3.1.1. The use, lease or sell of personal data

The use of data and the sale or lease of data for economic purposes is governed by § 28 of the Federal Data Protection Code. It is only admissible under certain additional circumstances. In its subsection 3 is listed under which circumstances a sale or lease of data to a third party is admissible. According to § 28(3) “the transfer or use of personal data for other purposes (other purposes means non public and non administrative purposes) if

1. it is done for the protection of legitimate interests of a third party

2. ...

3. for the purpose of advertising, marketing research and opinion research, if the personal data is filed in a list or compiled in that way that the persons affected are members of a certain group of persons that is limited to the following extend:
a) indicating the affiliation of the affected person to a specific group of persons,

b) occupational title, title of the industrial sector and the title of business,

c) the name,

d) title,

e) academic degree,

f) address, and

g) date of birth

The use of this data by private persons or companies is limited by § 28(4) of the Federal Data Protection Code\textsuperscript{143} as provision for the in § 28(3) mentioned type of data. In the case of § 28 (3) No.1 the trustee is allowed to sell the data to a third party which has legitimate interests in the data unless these interests are not the interests mentioned in §28(3) No.3. The legitimate interest is interpreted very broadly. These interests can also be to maintain this person as an e-costumer the third party’s business.

According to § 28(4) sentence 1 the selling company has a duty to inform the affected person before the data is sold to a third party. Then the affected person has consistent with § 28(4) sentence 2 of the Federal Data Protection Code the opportunity to “opt-out” and stop the sale of his individually identifiable data. This provision is applicable as long as no other provision sets higher requirements for the sale of this type of personal data. The legislator has made different provisions to safeguard the “opt-out” rule of § 28(4) and the “opt-in” rule of § 4(1) of the Federal Data Protection Code.

\textsuperscript{143} § 28(4) of the Federal Data Protection Code states: "The affected person has to be informed about the right to “opt-out” when the individual is approached for the purpose of advertising and marketing"
4.3.1.2 The rights of the affected person and claims for compensation

In § 6 of this code is ruled that the right to get information about the data stored of the affected person, the right to have this data blocked from trade, erased, or corrected can not be limited or excluded by a contractual obligation. These inalienable rights shall protect the affected person from being ripped off his privacy rights. Even if he discloses all of his personal data the affected person still maintains these rights to control the data circulating in the databases.\textsuperscript{144}

Further it is ruled according to § 7 of the Federal Data Protection Code the “affected person has a right to demand compensation” if someone violates the privacy rights of this affected person by collecting, processing or using personal data not in accordance with the Federal Data Protection Act or any other law protecting privacy issues. The party, which committed this, has to pay damages to the affected person. This is the central provision for a claim for damages when privacy rights are violated.\textsuperscript{145} Thus the affected person still may have secondary rights to claim for damages if terms and conditions of a contract are violated. These violations are seen as violations of secondary obligations and are based on contractual law.\textsuperscript{146} While also damages claim as tort is possible as a violation of the fundamental right of informational self-determination. This would be protected by § 823 subsection (1) of the German Civil Code\textsuperscript{147}, which can only be seen as catchall element and is subsidiary to the above-mentioned options.\textsuperscript{148}

\textsuperscript{145} Spiros Simitis “Bundesdatenschutzgesetz – Kommentar” [2003] at § 7 No. 56.
\textsuperscript{146} Spiros Simitis “Bundesdatenschutzgesetz – Kommentar” [2003] at § 7 No. 57.
\textsuperscript{147} German Civil Code of the 18\textsuperscript{th} August 1896, See Annex I.
\textsuperscript{148} Spiros Simitis “Bundesdatenschutzgesetz – Kommentar” [2003] at § 6 No. 7
These provisions safeguard that the rights of the affected person are observed and if his rights are harmed, he has the opportunity to get a financial compensation.

The Federal Data Protection Act also rules on the issue of a kind of “ombudsman”, this kind of profession has already been mentioned above in the Leahy-Hatch-Amendment. This “Datenschutzbeauftragter” – data protection officer shall on the one hand side report every second year if data protection issues have been disregarded and how data protection law has developed in the recent years. In line with § 26 BDSG the data protection officer can give recommendations to improve the current situation. If a case of sale of data that is not in accordance with the law the data protection officer has the opportunity to object the sale. The officer has the function of a watchdog but not the power to stop the sale or reverse it.

4.3.2 Special laws protecting privacy

The German codes also provide a higher degree of protection if the personal data is used for special purposes like advertisements. Also the codes provide certain rules if the data was gained in a special environment that demands a higher degree of protection.

The first aspect has not to be regarded by the trustee when he sells the data to a third party in the insolvency procedure, but has to be regarded by the third party. If the sale of data was for advertising purposes the buyer of the data has additionally ask for the consent to use the data for e-mails that contain advertisements. This “opt-in” rule can be found in § 4 of the Tele-Services Data
Protection Code “Teledienstedatenschutzgesetz”\textsuperscript{149} and in § 7 of the Tele-Services Code.\textsuperscript{150} These provisions are safeguarded by rules that allow the court or public administration to fine the one who violates the law a maximum of 50.000,- Euro per breach.

At last there is a provision of the German Criminal Code – “Strafgesetzbuch”\textsuperscript{151} that has effects on a sale of individually identifiable data in an insolvency. Especially § 203 of the German Criminal Code protects the sale of some special kind of data.

In § 203 Section 1 is ruled that someone “who reveals unauthorised secrets that belong to the personal sphere or are trade or company secrets can be sentenced to prison for a year or has to pay a fine”. These kinds of secrets have to be gained by a medic, dentist, veterinarian, apothecary or other member of the same kind of profession described. Also data collected by psychologists, gestational advisory services, family and related advisory services, lawyers, patent-lawyers, auditors and tax-consultants are protected. The provision use the term “unauthorised”, that means, that for example a trustee of an insolvent lawyer may sell the data of the clients only in the case he asked for permission prior to the sale. Following this there is an “opt-in” rule protecting the sale of individually identifiable data in some cases.

\begin{footnotes}
\item[149] Tele-Services Data Protection Code “Teledienstegesetz (TDDSG)” of the 22
\item[150] Tele-Services Code “Teledienstegesetz (TDG)” of the 14
\item[151] German Criminal Code “Strafgesetzbuch” of the 13
\end{footnotes}
4.3.3 Conclusion Data Protection Law

Codified law mainly regulates the German approach on privacy law issues. This law does not give the private enterprises the space to design own codes of good conduct or privacy policies, which may allow an easier trade of data. Even in an insolvency procedure a receiver has to regard several different provisions of different codes if he wants to sell the individually identifiable data in this procedure to maximise the financial benefits. The German codes are mainly influenced by the EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and the Directive 1995/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This also would influence the sale of data in an insolvency if the database would be sold across the borders of the EU. The most interesting case is the sale of data from an insolvent German company to a buyer that has the place of incorporation in the United States of America. This sale from a country with a highly codified protection of privacy to a country with a self-regulatory approach is critical. In line with § 4b(3) of the Federal Data Protection Code a transfer into a non-EU country this country has to guarantee an adequate level of protection. This provision is based on Article 25 the Directive 1995/46/EC.\(^{152}\)

\(^{152}\) Art. 25 of Directive 1995/46/EC states that “The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection.”
5. Chapter 5 - Legal conflicts that can arise from an interaction

The German legal system has transposed the above mentioned Directive 1995/46 and allows the export of personal data under two premises set up by the Directive which can also be found in § 4b(3) of the Federal Data Protection Code. The first premise is the contractual protection of personal data; the second premise is that the jurisdiction to which the data is exported has laws that safeguard an adequate protection.

In the beginning the problem arose that the USA did not provide an adequate level of protection and thus the transfer would have been illegal. This would have been a sever problem for the economies on both sides of the Atlantic. In 1998 the USA started to discuss how they could ensure the data exchange with the EU and developed the idea of the “Safe Harbour.” This policy should safeguard the premises of the EU law in a self-regulatory framework made by US companies. US companies set up certain principles on data protection and enterprises which fulfil the demands stemming from these major principles could receive and process personal data of EU citizens. The Commission approved the agreement. The main principles of the “Safe Harbour” policy are as follows:

The organisations that join the “Safe Harbour” must provide individuals with information that is framed as a notice in a “clear and conspicuous language.” This notice has to be given at the time when the data is collected. It has to contain information on how the data is going to be used or to which third party it

154 Ibid.
155 http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited at the 7th September 2004).
may be disclosed.\textsuperscript{156} Secondly the individual has to have the choice to “opt-out” of the compilation of data either if the data is disclosed to a third party or used for an incompatible use. Thirdly there is an “opt-in” rule for individuals if the processing company wants to transfer the data to a third party. This third party has to have subscribed to the “Safe Harbour.”\textsuperscript{157} The data processing companies have to take reasonable precautions to protect the security of the personal information against loss, abuse, and unlawful access, disclosure, alteration and destruction.\textsuperscript{158} The enterprise has to provide affected persons with the opportunity to access any personal information held. And if the affected person objects the data, the enterprise has to give this person the opportunity to correct, amend, or delete that personal information when it is inexact. Further the personal data has to be relevant for the purpose for that it is used. An external organisation should ensure the so-called “Data integrity” which means that the personal data is reliable for its intended use, accurate, complete, and current.\textsuperscript{159} Last but not least there has to be an enforcement mechanism provided to resolve complaints in a dispute resolution system.\textsuperscript{160}

The receiver in a German insolvency procedure has to proof that the US company participates in the “Safe Harbour” and thus the individually identifiable data sold is protected in an adequate form. Otherwise the receiver would be liable according to § 60 of the German Insolvency Code is the receiver liable for losses and damages suffered by third parties “if he is lacking the due diligence of

\textsuperscript{156} Ibid.
\textsuperscript{157} Ibid.
\textsuperscript{158} Ibid.
\textsuperscript{159} Ibid.
\textsuperscript{160} Ibid.
a proper and assiduous receiver. Thus if the data is sold by the receiver in an insolvency proceeding the interests of the e-costumer are protected by the German legal system by a bigger extend.

6. Chapter 6 - Conclusion and method of resolution on the outlined problem

The different approaches of the EU and the United States to data protection, privacy and insolvency law have framed two very different legal systems within the last century. These laws reflect the forms of social evolution and market economy development. The two relevant issues for this paper are the following:

While the US system prefers the ideal that the private persons and their businesses shall underlie their self-regulation and laws in some sectors that need a special protection the EU prefers to use legislative measures and governmental interference.

While the US only know privacy as a principle that can be derived from several amendments of the US Constitution. And even this principle is attacked by the e-retailing industry with the Constitution by arguing that the right to free speech would invoke a right to transfer thus sell data. Thus the Supreme Court once judged that an advertisement could not be seen on the level of free speech the affected person has to have the choice if he wants to receive advertisements. This was the birth of the American “opt-out” system.

The EU and especially Germany have developed several laws to protect privacy to a great extend. Thus privacy is seen as human right in Europe that can also be

161 § 60(1) Sentence 2 of the German Insolvency Code.
found in Article 1 of the Directive 1995/46. In Germany privacy is derived from the Article 2(1) in connection with Article 1 of the German Basic law.

These two general problems can also be seen in the legislation on bankruptcy issues while the German law has no problems to identify individually identifiable data as intangible property that underlies a special protection and a limited alienability the US legal system still has problems to characterise this type of data. On the data protection side the USA has developed a system of “opt-out” choices to ease the trade and free flow of data and have a minimum of administrative costs. This system is even constituted in the Gramm-Leach-Bliley Act on the exchange of financial data.

The continental European system prefers the “opt-in” version to give a maximum of protection to the e-costumer. These two different systems have also an effect on the bankruptcy procedure while in the EU a general “opt-in” clause is used in an insolvency and the German law mainly uses the “opt-in” system in the first step when the data is collected and in the most cases the “opt-out” when the data is sold in an insolvency to protect the fundamental right the US has until today no general approach on this matter. Neither the U.S. Bankruptcy Code nor the data protection codes provide a consistent method to protect the e-costumers.

To find a method to fill the gap between these approaches is very difficult as can be seen above. As long as these to completely different systems do not interact there is no problem at all, but in the case that the data is sold in insolvency procedure across this border a solution has to be found. As seen above, the United States developed the Safe Harbour principle to solve this problem. Although this system is criticized by privacy lawyers and the Art. 29 Working
The accord is based on a system of self-regulation without governmental influence. The participating enterprises only promise not to violate their declared privacy practices. The enforcement mechanisms are few. The Art. 29 Working Group concluded in its 62nd paper that all essential elements of the Safe Harbour Agreement are in place and that a structure for individuals to bring forward complaints exists. The Working Group however did not find a sufficient transparency of the participating companies. Further not all providers of a dispute resolution complied with the principles of the agreement. Also the change of the privacy policies by Amazon.com and ebay.com as a result of the Toysmart.com insolvency to the detriment of their costumers has to be regarded in the future. These cases show that the self-regulation approach used in the United States can only work, if the companies have to fear massive costs coming up if they do not comply. This principle of commerce is the only way to enforce the self set standards while otherwise the incentive to breach the own rules is too big. A legislative action of the federal government could create this incentive. The control mechanisms already installed are only working in some fields. The FTC for example can interfere in the case that an e-retailer breaks the own privacy policy in the case of bankruptcy. And thus acts in a deceptive practice or fraudulent way. Also the FTC can only act when a special law is

165 See above.
166 See also D. Ian Hopper, “Groups criticise Amazon policy” AP online 1st September 2001, available at Westlaw UK at 2000 WL 25992933.
broken like the COPPA or Gramm-Leach-Bliley Act. Thus stronger enforcement mechanisms are necessary.

The “opt-in” procedure which is promulgated by the EU legislation and also by the German legislation is preferable to the US “opt-out” system for several reasons that not only has a positive effect for the e-customer. On the e-customer protection side it can be stated that an “opt-in” guarantees a maximum protection of the privacy interests. The “opt-in” system would give the e-customer the opportunity to develop an ability to value their data and the risk of disclosure.167 While the “opt-out” system does not and even further companies to have a confirmation that the e-customer still exists may abuse it. The “opt-in” variant is also a benefit for the party purchasing the data because they are going to buy only data of clients that are interested in taking up business relations with the buyer or are likely to receive further information. And at last the “opt-in” is positive for the selling company the value of a set of personal data of a client who is interested in contacting the buyer may gain more money for each set of data. Even according to the cost minimizing approach of a property-supporting fraction of academics the “opt-in” solution would not create further costs for the selling party or the buyer. The seller only has to send an e-mail to each of his customers and give a deadline until the e-customers shall have agreed to the sale and reply to the e-mail.

This leads to the most complex problem the characterisation of individually identifiable data in the US legal system. It would be the best if the federal government would find a fitting rule while the current situation is not satisfying

at all. Even according to the US approach of self-regulation there is need to find a solution for this problem. The Leahy-Hatch Amendment was a good solution in this field and pointed the way towards a property-based solution.

This property-based solution should limit the alienability of individually identifiable data like the EU already did for sensitive data and the inalienability of rights to erase or correct incorrect data. All these measures would enhance the protection of e-costumers in bankruptcy without changing the legal approach of the US legal system. The change has to be made to a balanced and fair game between the participating parties, otherwise individually identifiable data would be treated as fair game.
Bibliography:

Books and Articles:


Bergelson, Vera “It’s personal but is it mine? Toward property rights in personal information” [2003] 37 U.C. Davis L. Rev. 379


Countryman, Vernon “Executory Contracts in Bankruptcy” [1972] 57 Minn. L. Rev. 439

Edwards, Lillian “Consumer privacy, on-line business and the Internet: Looking for privacy in all the wrong places” [2003] 11 IJL&IT 226


<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hopper, D. Ian</td>
<td>“Groups criticise Amazon policy”</td>
<td>AP online 1st September 2001, available at Westlaw UK at 2000 WL 25992933</td>
</tr>
<tr>
<td>Janger, Edward</td>
<td>“Muddy property: Generating and protecting information privacy norms in bankruptcy”</td>
<td>[2003] 44 Wm. &amp; Mary L. Rev. 1801</td>
</tr>
<tr>
<td>Janger, Edward</td>
<td>“Privacy property, information costs, and the anticommons”</td>
<td>[2003] 54 Hastings L. J. 899</td>
</tr>
</tbody>
</table>
Lipson, Jonathan  “Financing information technologies: Fairness and function”, 2001 Wis. L. Rev. 1067


Martin, Craig  “Mailing lists, Mailboxes and the Invasion of Privacy: Finding a contractual solution to a transnational problem” [1998] 35 Hous. L. Rev. 801

Merrill, Thomas W. & Smith, Henry E.  “Optimal Standardisation in the law of property” [2000] 110 Yale L. J. 1


Nguyen, Xuan-Thao N. “Collateralising Privacy”, [2004] 78 Tul. L. Rev. 553


Schwartz, Paul M. “Property, privacy and personal data” [2004] 117 Harv. L. Rev. 2055
<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
<th>Year/Publication Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shavell, Steven</td>
<td>“The judgement proof problem”</td>
<td>[1986] 6 Int’l Rev. L. &amp; Econ. 45</td>
</tr>
<tr>
<td>Usmani, Farah</td>
<td>“Information privacy and Internet company insolvencies: When a business fails, does divestiture or bankruptcy better protect the consumer?”</td>
<td>[2003] 8 Fordham J. Corp. &amp; Fin. L. 273.</td>
</tr>
<tr>
<td>Warren, Samuel &amp; Brandeis, Louis</td>
<td>“The right to privacy”</td>
<td>[1890] 4 Harv. L. Rev. 293</td>
</tr>
<tr>
<td>Weichert, Thilo</td>
<td>“Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung”</td>
<td>[2001] NJW p. 1463</td>
</tr>
</tbody>
</table>

Working Paper of the Art. 29 Working Group,
“Working Document on the functioning of the Safe Harbour Agreement

Working Paper of the Art. 29 Working Group,
Table of cases:

Avery Dennison Corp. v. Kitsonas, [2000] 118 F. Supp. 2d 848


Decision of the Federal Constitutional Court of the 15th December 1983, BVerfGE 65, p. 1 so called “Volkszählungsurteil – judgement on the population census”


In re Leckie [1996] 99 F.3d 573

In re Qintex Entertainment Inc., [1991] 950 F.2d 1492

In Re: Toysmart.com, LLC, No. 00-13995-CJK

Integrated Solutions Inc. v. Service Support Specialists Inc, 124 F.3d 487; see also Bishop College, [1993] 151 B.R. 394


ProCD Inc. v. Zeidenberg, [1996] 86F.3d 1147

Sipes v. Atlantic Golf Communities [1996] 84F.3d 1364

Table of Statutes:

Constitution of the United States of America of the 4th July 1776

Federal Basic Law of the Federal Republic of Germany of the 23rd May 1948


Directive 1995/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Civil Code of the 18th August 1896, last revision of the 15th July 2002

Council Regulation No. 44/2001 of 22nd December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters

Council Regulation No. 1346/2000 of 29th May 2000 on insolvency proceedings

Childrens Online Privacy Protection Act of 1998, Title 15 USCA §§ 6501 – 6508

FTC Act of 1914, Title 15 USCA
US Bankruptcy Act of 2000, Title 11 USCA Chapter 11

Gramm-Leach-Bliley Act of 1999, Codified in different Sections 12 and 15 of the USCA

“Can-Spam” Act of 2003, Title 18 Chapter 46

Federal Data Protection Code – Bundesdatenschutzgesetz of the 14th January 2003


German Criminal Code “Strafgesetzbuch” of the 13th November 1998

Insolvency Code of the 1st January 1999, last revision at the 5th April 2004

Tele-Services Code “Teledienstegesetz (TDG)” of the 14th December 2001, formerly known as Informations- und Kommunikationsdienstegesetz (IuKDG)

Tele-Services Data Protection Code “Teledienstegesetz (TDDSG)” of the 22nd July 1997 last amended at the 14th December 2001

Planned Leahy-Hatch Amendment, S. 420, 107th Congress § 231(a)(1)(B)

Planned Bankruptcy Reform Act of the 108th Congress

Table of websites cited in the dissertation:

http://www.wired.com/news/business/0,1367,37517-2,00.html
Annex I – Texts of some Laws and Statutes used

§ 361. Adequate protection

When adequate protection is required under section 362, 363, or 364 of this title of an interest of an entity in property, such adequate protection may be provided by--

(1) requiring the trustee to make a cash payment or periodic cash payments to such entity, to the extent that the stay under section 362 of this title, use, sale, or lease under section 363 of this title, or any grant of a lien under section 364 of this title results in a decrease in the value of such entity's interest in such property;

(2) providing to such entity an additional or replacement lien to the extent that such stay, use, sale, lease, or grant results in a decrease in the value of such entity's interest in such property; or
granting such other relief, other than entitling such entity to compensation allowable under section 503(b)(1) of this title as an administrative expense, as will result in the realization by such entity of the indubitable equivalent of such entity's interest in such property.

§ 363. Use, sale or lease of property

(a) In this section, "cash collateral" means cash, negotiable instruments, documents of title, securities, deposit accounts, or other cash equivalents whenever acquired in which the estate and an entity other than the estate have an interest and includes the proceeds, products, offspring, rents, or profits of property and the fees, charges, accounts or other payments for the use or occupancy of rooms and other public facilities in hotels, motels, or other lodging properties subject to a security interest as provided in section 552(b) of this title, whether existing before or after the commencement of a case under this title.

(b)(1) The trustee, after notice and a hearing, may use, sell, or lease, other than in the ordinary course of business, property of the estate.

(2) If notification is required under subsection (a) of section 7A of the Clayton Act in the case of a transaction under this subsection, then--

(A) notwithstanding subsection (a) of such section, the notification required by such subsection to be given by the debtor shall be given by the trustee; and

(B) notwithstanding subsection (b) of such section, the required waiting period shall end on the 15th day after the date of the receipt, by the Federal Trade Commission and the Assistant Attorney General in charge of the Antitrust Division of the Department of Justice, of the notification required under such subsection (a), unless such waiting period is extended--

(i) pursuant to subsection (e)(2) of such section, in the same manner as such subsection (e)(2) applies to a cash tender offer;

(ii) pursuant to subsection (g)(2) of such section; or

(iii) by the court after notice and a hearing.

(f) The trustee may sell property under subsection (b) or (c) of this section free and clear of any interest in such property of an entity other than the estate, only if--

(1) applicable nonbankruptcy law permits sale of such property free and clear of such interest;

(2) such entity consents;

(3) such interest is a lien and the price at which such property is to be sold is greater than the aggregate value of all liens on such property;

(4) such interest is in bona fide dispute; or
such entity could be compelled, in a legal or equitable proceeding, to accept a money satisfaction of such interest.

§ 365. Executory contracts and unexpired leases

(a) Except as provided in sections 765 and 766 of this title and in subsections (b), (c), and (d) of this section, the trustee, subject to the court's approval, may assume or reject any executory contract or unexpired lease of the debtor.

(b)(1) If there has been a default in an executory contract or unexpired lease of the debtor, the trustee may not assume such contract or lease unless, at the time of assumption of such contract or lease, the trustee--

(A) cures, or provides adequate assurance that the trustee will promptly cure, such default;

(B) compensates, or provides adequate assurance that the trustee will promptly compensate, a party other than the debtor to such contract or lease, for any actual pecuniary loss to such party resulting from such default; and

(C) provides adequate assurance of future performance under such contract or lease.

…

(d)(1) In a case under chapter 7 of this title, if the trustee does not assume or reject an executory contract or unexpired lease of residential real property or of personal property of the debtor within 60 days after the order for relief, or within such additional time as the court, for cause, within such 60-day period, fixes, then such contract or lease is deemed rejected.

…

(f)(1) Except as provided in subsection (c) of this section, notwithstanding a provision in an executory contract or unexpired lease of the debtor, or in applicable law, that prohibits, restricts, or conditions the assignment of such contract or lease, the trustee may assign such contract or lease under paragraph (2) of this subsection; except that the trustee may not assign an unexpired lease of non-residential real property under which the debtor is an affected air carrier that is the lessee of an aircraft terminal or aircraft gate if there has occurred a termination event.

(2) The trustee may assign an executory contract or unexpired lease of the debtor only if--

(A) the trustee assumes such contract or lease in accordance with the provisions of this section; and

(B) adequate assurance of future performance by the assignee of such contract or lease is provided, whether or not there has been a default in such contract or lease.

(3) Notwithstanding a provision in an executory contract or unexpired lease of the debtor, or in applicable law that terminates or modifies, or permits a party other than the debtor to terminate or modify, such contract or lease or a right or obligation under such contract or lease on account of
an assignment of such contract or lease, such contract, lease, right, or obligation may not be terminated or modified under such provision because of the assumption or assignment of such contract or lease by the trustee.

(2) The trustee may assign an executory contract or unexpired lease of the debtor only if--

(A) the trustee assumes such contract or lease in accordance with the provisions of this section; and

(B) adequate assurance of future performance by the assignee of such contract or lease is provided, whether or not there has been a default in such contract or lease.

(3) Notwithstanding a provision in an executory contract or unexpired lease of the debtor, or in applicable law that terminates or modifies, or permits a party other than the debtor to terminate or modify, such contract or lease or a right or obligation under such contract or lease on account of an assignment of such contract or lease, such contract, lease, right, or obligation may not be terminated or modified under such provision because of the assumption or assignment of such contract or lease by the trustee.

Draft of the Bankruptcy Reform Act of the 107th Congress S.420

SEC. 231. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(a) IN GENERAL- Section 363(b)(1) of title 11, United States Code, is amended by striking the period at the end and inserting the following: `except that if the debtor has disclosed a policy to an individual prohibiting the transfer of personally identifiable information about the individual to unaffiliated third persons, and the policy remains in effect at the time of the bankruptcy filing, the trustee may not sell or lease such personally identifiable information to any person, unless--

`(A) the sale is consistent with such prohibition; or
`(B) the court, after notice and hearing and due consideration of the facts, circumstances, and conditions of the sale or lease, approves the sale or lease.'

§ 103 Choice of the receiver – German Insolvency Code

(1) If there is a reciprocal contract at the time of the filing of the insolvency procedure of the debtor and of the other part not yet fully fulfilled, the appointed receiver can demand the fulfilment of the contract and fulfil the contract.
(2) Does the receiver reject the fulfilment, then the other part can claim for damages resulting from the non-performance. He will be treated then like an unsecured creditor.

§ 153 Statement of assets and liabilities – German Insolvency Code

(1) The receiver has to compile in the moment of the filing of the insolvency an overview, in which all the assets and liabilities of the insolvent entity have to be listed in the form of a balance sheet.

§ 4a Consent – Federal Data Protection Code

(1) The consent of the affected person is only valid, if it is based on the free will of the person. The person has to know the purpose of the inquiry, processing or use.

§ 7 Compensation – Federal Data Protection Code

If an affected person suffers a damage by a person in charge in so far that his data was collected, processed or used in an inappropriate way, infringing the Federal Data Protection Code or any other code protecting privacy issues then the person in charge has to pay a compensation for the damage caused. The liability to pay damages is obsolete when the person in charge acted with due diligence.

§ 823 subsection (1) of the German Civil Code

Someone who violates intentionally or negligently life, the integrity of the body, the health, the liberty, the property or another right of another person, has to compensate the caused damage.

Annex II – Definitions

Cookies are defined by Prof. Kurtz in Leslie A. Kurtz, “The invisible becomes manifest: Information privacy in the digital age” [1998] 38 Washburn L. J. 151 as:

Small data files deposited on your hard disk drive by a site you are visiting. When you connect to a web-site that uses cookies, the web-site computer, called a web-server, deposits a the cookie – a small piece of information about your visit to that site – and a unique identifier on your computer’s hard disk drive. The next time you visit the site, the cookie is transmitted back to the web server,
which than can “remember” what you did last time. The information can be stored in a database and can be used to customise the site or to target advertisements or content. Cookies allow web site operators, including advertisers, to record information such as the trail of sites that a person visits and her online purchases, often without her knowledge. For example the operator of a site that sells books or videotapes can know every web page that the user has clicked on at every book or film looked at or ordered over a number of visits, allowing the operator to compile a list of the user’s preferences.

“personally identifiable information” would have been defined by the draft Bankruptcy Reform Act of the 107th Congress (S.420) as the individual’s first name (or initials) and last name, whether given at birth or adoption or legally changed; the physical address for the individual’s home; the individual’s e-mail address; the individual’s home telephone number; the individual’s social security number; or the individual’s credit card account number; and means, when identified in connection with one or more of the items of information listed above – an individual’s birth date, birth certificate number, or place of birth; or any other information concerning an identified individual that, if disclosed, will result in the physical or electronic contacting or identification of that person.

TRUSTe describes itself on the homepage www.truste.com as an independent, non-profit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. … We were founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium to act as an independent, unbiased trust entity. The TRUSTe privacy program – based on a branded online seal, the TRUSTe "trust mark" – bridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards.