Panikos Fakontis
Law Degree in University of Thrace (Greece)
LLM Leicester (U.K)
The author can be contacted by e-mail at fakontis@yahoo.com

**What might discourage consumers from engaging in e-commerce? How far can the law go in solving the relevant problems?**

Electronic commerce may be defined as the production, advertising, sale and distribution of products via telecommunication networks[1]. Before a consumer enters into an electronic transaction there are three stages that could be distinguished; firstly, the searching stage, secondly, the ordering and payment stage and thirdly the delivery stage[2]. Each of the above stages involves many reasons that might discourage a consumer to engage finally into a transaction. Thus, legislators have to regulate the existing problems in order to give to consumers the confidence to interact and enter into e-commerce transactions but also teach the sellers of how they can perform[3].

The creation of internet created a global market that needs to be adequately regulated. The way to be achieved is the international cooperation; moreover, if coordination is fulfilled at a certain level then concurrently enforcement of claims will be reached. The Council of Europe Convention on Cybercrime[4] attempts an international harmonization in this area and includes *inter alia* offences against the confidentiality, integrity and availability of computer systems, such as illegal access, illegal interception, data interference, and moreover computer related offences such as forgery and fraud[5].

[1] Bacchetta M et al, "Electronic *commerce and the role of the WTO*" World Trade Organisation, Special studies 1998, at 1.
[2] Ibid.
[3] Reed C and Angel J "*Computer Law*" (5th edn Oxford 2003), at 352.
[4] Convention on Cybercrime, Nov, 23, 2001,Europ.T.S.No 185. http://conventions.coe.int/Treaty/en/Treaties/Hunl/185.htm Convention on Cybercrime>.
[5] Flanagan A, "*The law and computer crime: Reading the script of Reform"* 13(1) International journal of Law and information Technology, Oxford University Press, 2005, at 100.

Consumers sometimes have many doubts before buying online since the potential risk of loosing their money is quite high and pushes them back to their local shops with the higher prices in the goods. Internet nowadays allows consumers to buy goods from a wide section of sellers from all over the world and that benefits competition and finally has effects on the product's price. Consumers can easily get the products that they desire in better prices and sometimes in a better quality because they have the opportunity to use internet search engines, compare and then decide what is suitable to their needs. Moreover, the EU adopted among others the distance selling directive in order to protect consumers' interests by obliging sellers to comply with certain standards[6].

However, there are problems that undermine the above mentioned advantages; the most serious current threat is the infringement of privacy[7]. When consumers are shopping online their personal data are being stored and most of the times without their consent and knowledge. That practice raises questions such as how personal data are used, for what purpose, what if they sell their databases to others and what will happen if a third party manages to have illegal access to their database of consumer's personal data? These questions can deter consumers from engaging into e-commerce. European Union entered a directive[8] on data protection but the question is whether it is enough and enforceable?

This paper is concerned with the problems of fraud and privacy. It will commence with the problem of fraud and it will continue with the problem of intrusion to privacy because of the creation of personal information databases. In each part it will be made an attempt to propose changes that are need to be done to the European Union Directives and also suggestions of who far can the Law in solving those problems.

## **Fraud.**

The American chairman of the House subcommittee on crime stated that: "America must protect our national security critical infrastructure and economy

[6] Directive 97/7/EC.
[7] Edwards L, "*Consumers privacy, On-Line Business and the Internet: Looking for privacy in all the Wrong Places*" 11(3) International Journal of Law and Information Technology 2003 at 227.
[8] Directive 95/46/EC.

from cyber attacks. Penalties and law enforcement capabilities must be enacted to prevent and deter such criminal behaviour. Until we secure our cyberspace infrastructure, a few keystrokes and an internet connection is all one needs to disable the economy or endanger lives. A mouse can be just as dangerous as a bullet or a bomb[9]". Smith's comment has implications not only for America but for any country. From his speech it is worth noting the negative effects of cyber attracts on economy. Consumers' main fear when engaging in e-commerce transactions is fraud. The crime of fraud can be committed by many ways, such as by setting up a website of non-existence and in this way the consumer will give his money but will never receive his order; another way is by obtaining personal data such as the cardholder's number and using it in the future without authorization for obtaining their money. The elements of the crime of fraud are basically the theft of property by trickery or deception and when using the internet for shopping, the crime can be committed easier, across many borders, with more potential victims[10]. Computer is simply a modern tool[11].

Computer fraud is a serious obstacle for customers before engaging into e-commerce. The English Audit commission defined the term computer fraud and stated that is "any fraudulent behaviour connected with computerisation by which someone intents to gain financial advantage[12]. There are various types of Internet fraud such as misuse of credit cards, failure to deliver goods ordered and paid for, pyramid selling[13]. The most significant is credit card misuse and especially where retailer's database has been accessed by hackers and then published on the internet for use by anyone.[14] Moreover threats to electronic security and fraud can arise from internal and external sources[15]. Internal sources could be the employees of a business, who as insiders have access to their databases. It's noteworthy that 25% of all computer frauds are committed by someone in authority within the

[9] Smith L, chairman of the American House of the Subcommittee on crime. Hearing on H.R 3483.
[10] Flanagan, n 5 above, at100.
[11] Reed, Angel, n 3 above, at 296.
[12] Audits Commission's surveys. See Lloyd I, " *Information Technology Law*" (4th edn 2004, Oxford), at 270.
[13] Lloyd, n 12 above, at 273.
[14] Ibid.
[15] Esen R, "*Cyber Crime: A crowing problem*", journal of criminal law, 2002, at 2.

company[16]. External sources could be those groups or individuals who obtain unauthorized access to computer systems[17].

A distance selling contract requires payment by credit or debit card but there is always the danger of misuse of the cards details. The consumer in order to place an order has to give the numbers and usually the expiry date of the card and thus authorises the seller to withdraw money. However there is the danger of hacking the cards' numbers from a third party and by obtaining them can enter into transactions and charge the cardholder. Moreover, the payment has to be in advance and that is what exposes consumers to the risk of fraud; if prepayment was not required the risk could be minimized thus the law should impose that payment will have to take place after the consumer's confirmation of the order.

The abstraction of the card's details is the main fear of many consumers. The law should provide limitations of diligent consumer's liability to a certain amount in order to attract them into e-commerce. The Commission of Europe has issued a recommendation concerning transactions by electronic payment instruments and in particular between issuer and holder[18]. The recommendation intents to promote customers' confidence and a higher level of consumer protection in e-commerce[19]. Thus, it sets out minimum requirements concerning the obligations and liabilities of the parties involved. Moreover, Article 5 provides that the card holder shall bear the maximum liability of 150 Euro. The recommendation should be incorporated in an obligatory legal text for all member states and maybe from countries outside EU because internet market is without any borders. Furthermore it should be noted that the American companies Visa and MasterCard are advertising, the slogan "Zero Liability" for any unauthorized transaction[20].

Lawmakers should enact provisions that would oblige banks to adopt higher security measures in order to prevent abstraction of card information. A

[16] Law society "News-*Campaign for computer hacking law escalates*" Law society's Guardian Gazette 1989.
[17] Esen, n 15 above, at 2.
[18] Directive 97/489/ EC.
[19] Directive 97/489/EC recital 4, 8.
[20] http://www.cardoffers.com/reviews/cards/details/card.asp?id=423, at the terms and conditions.

possible solution could be the adoption of the SSL (Secure Sockets Layer) that they encrypt card's information and it becomes almost impossible to decrypt them.[21]Law loses value and justification if it is not complemented by other forms of protection such as security and consumer education[22].

Another existing problem that can discourage consumers from shopping from internet is Phishing[23]. Phising is the most recent form of identity fraud and the word comes from an analogy to fishing, the "f" is changed to "ph" in keeping with computer hacking tradition[24]. The most common feature of that method of fraud is by sending an email that looks like it is from a bank or e-commerce site by using its logos or trademarks and gives warnings and threats such as account closure or problem; by that the user logs on his bank's site for instance (gives his name, security password, account number) and thus the sender or "fisher" obtains all necessary information needed to defraud. That method contributes to the loss of consumer confidence in conducting business online[25]. Moreover, once a thief has obtained personal information, he can open new credit accounts, run up bills etc. Phishing is so dangerous that can discourage consumers from engaging into net shopping; the anonymity that exists on the internet, and the usage of multiple ISPs by them makes it very difficult to be caught by the authorities[26]. In respect to these facts someone would wonder if internet should still be anonymous. The law should establish strict public law in order to punish such criminals when arrested but at the same time there is a need for the creation of groups of experts that they will be able to trace them and bring them to justice. Moreover, in order to achieve punishment should lower the required level of intent.

The European Commission in order to deal with fraudulent use of the card numbers and also give incentives to consumers for engaging into e-commerce, created a committee to deal with the "chargeback" concept when paying over

[21] Aleksandridou E, "*The law of e-commerce*", (Greek),( 2004, Sakkoulas), at 79.
[22] De Cock Buning et al "*consumer@ protection. E.U. An analysis of European consumer legislation in the information society"*, 3-4 Journal of Consumer policy, at 289.
[23] Lynch J, "Identity *Theft in Cyberspace: Control methods and their Effectiveness in Combating Phising attacks*" 20 Berkeley Technology Law journal, 2005, at 259.
[24] Ibid.
[25] See Introduction of the anti-Phising Act of 2004 available at:http://leahy.senate.gov/press/200407/070904c.html.
[26] Lynch, n 23 above, at 272.

Internet[27]. That concept is a refunding of the payment transactions made via internet and it is very well known in the USA which is more oriented towards consumer satisfaction and the merchant will refund without hesitation regardless of the nature of the problem in order to preserve his client[28]. The concept of chargeback is a measure friendly to the consumer and the law should establish that in the consumer's rights. A consumer will not be reluctant to enter into an e-commerce transaction when there is a statutory right of refund when he/she is not satisfied.

The introduction of the EEJ-NET[29] (European Extra Judicial Network) should be welcomed but at the same time is not advertised enough; it is a network of out of court redress mechanism and provides communication support to consumers. However the commission released a final document for e-commerce and financial services[30] and suggests the creation of cyber court; such a movement would be a positive movement in order to built consumer's confidence in e-commerce and solve the existing problems. Furthermore, if it was an on-line out of court dispute settlement could give access to justice[31]. For instance in England there is the possibility for online trial for small amount money claims[32].

**Distance Selling directive- Are European consumers adequately protected?**

The European Community in order to protect the consumers adopted the distance selling directive[33]. The directive is of minimum harmonisation but however member states are allowed to prescribe more stringent rules[34]; because of that member states in order to achieve more protection they should establish

[27] MARKT/173/2000 The European Commission, Working Document, Payment card chargeback when paying over internet. Available at: http://europa.eu.int/comm/internal_market/en/ecommerce/chargeback.pdf#search='173/2000%20chargeback'.
[28] The European Commission, *Working document, "Payment card Chargeback when paying over the internet*" 173/2000, at 8.
[29] Available at: http://www.eejnet.org/
[30] Available at: http://www1.ukie.gov.pl/sl/Rynek/7.pdf#search='com(2001)%2066%20final'.
[31] De cock Buning, n 22 above, at 309.
[32] https://www.moneyclaim.gov.uk/csmco2/index.jsp.
[33] 97/7/EC of the European parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts. OJ L 144,4-6-1997, at 19.
[34] Schaub M, *" European Legal Aspects of e-commerce"*, (Europa Law Publishing, 2004), at 79.

higher standards than the directive does. For instance Greece, when implemented the directive gave statutory protection for the right of cooling of period of 10 working days instead of seven and Germany gave for the same right two weeks[35]. The scope of the directive is not particularly e-commerce but is more broad covering contracts concerned with goods or services when are concluded at a distance between a consumer and a supplier[36].

The directives' main provisions could be summarized as follows: articles 4 and 5 impose an obligation on the supplier to provide to the seller certain information[37] prior the conclusion of the contract and a written confirmation of information in good time during the performance of the contract; article 6 gives the right to the consumer to withdraw within seven days from the day he/she receives the goods without a penalty; article 7 provides for the contract's performance and obligates the seller to execute the consumer's order in a period of 30 days and if he fails to do so because of unavailability of the goods or services he has to inform and return any payment made to the consumer; article 8 deals with payment by card and provides for the cases where a fraudulent payment was made, the consumer's payment card should be re-credited; article 16 obliges member states to inform consumers for their rights.

The consumer protection provided by the distance selling directive establishes the minimum standards[38] but there are some weak points that should be taken into consideration in a later reform in order to achieve higher protection. Article 3 exempts online auctions from its scope; companies such as eBay are very popular to consumers and as was reported by the credit card company Visa in 1999 one of the main grounds of disputed payments in Europe was for payments through internet based auctions[39]. The high popularity of such auctions obliges legislators to protect consumers thus it seems inappropriate to have such an exception. Moreover key provisions (such as articles 4, 5, 6 and 7(1)) can not

[35] Lodder A, "*eDirectives: Guide to European Union Law on E-Commerce*",( 2002, Kluwer Academic Publishers), at 18.
[36] Schaub, n 34 above, at 79.
[37] Lodder, n 35 above, at 14.
[38] Article 14 of the 97/7/ EC Directive.
[39] Lodder, n 35 above, at 13.

applied to consumer's booking online for accommodation and transport[40]; the reason of such an exception could be that the price is debatable on the date of booking nonetheless the weak party should be fully protected.

As noted above the directive on distance obliges the seller to give information of the goods and services before and during the contract's performance. However when it comes to supplying information, computer code or software, it is not clear from the directive whether these are treated as either services or goods, thus it needs to be clarified because it has very wide reaching consequences especially on the right of withdrawal[41]. Another issue is that the consumer has to pay the direct cost of returning the goods even when are supplied defective goods or goods which were not ordered[42], it can be fairly argued that the seller should bear the cost because it was his/her fault.

The distance selling directive is one of the key pieces of legislation. It impacts on the way in which a website is designed and provides a high level of protection, however there is a need for further legislation especially on enforcement and also dealing with small claims.

**European Convention on Cyber-crimes: A chance for international protection.**

The council of Europe also has formulated a convention on cyber-crimes and it is an attempt to harmonize countries' legal systems in order to include all types of fraud; thus it avoids the concept of deception in order to be more flexible and easier to convict the wrongdoer[43]. The Convention contains a mechanism whereby other countries outside EU can sign and ratify it[44]. Moreover, it deals with issues of substantive and procedural criminal rules and distinguishes the crimes into three categories;(1) offences against confidentiality, integrity, and availability of computer data and systems( illegal access, illegal interception, data interference, misuse of devices),(2) computer related offences (fraud, forgery), (3)

[40] Schaub, n 34 above, at 82.
[41] Lodder, n 35above, at 18. Also Reed and Angel, n 3 above, at 353.
[42] Lodder, n 35 above, at 20.
[43] Read and angel, n 3 above, at 297.
[44] Read and Angel, n 3above, at 315.

content related offences (child pornography and copyright protection)[45]. The convention is probably the most significant in the area of computer crime, and could be the best way of eliminating computer related crimes.

## Privacy

A U.S judge, Judge Cooley defined privacy as "the right to be let alone"[46]. Privacy is a prerequisite for the encouragement of consumers to engage themselves in e-commerce[47]. When we engage into an electronic transaction we have to leave our personal information and thus they are stored in databases. In that way commercial entities can process them and they can draw conclusions about the consumers' habits, financial situation and about the consumers' personality in general[48]. The collection and storing of consumers' data is usually either with our consent or without[49]; having such information helps them on their design of commercial strategies and finally creating more needs to the consumers.

Databases containing personal data are of enormous commercial value and can be sold for very high prices. For example Egghead software had a database containing information for about 4 million consumers and it was sold for 10 million dollars[50]. The above example illustrates the importance of storing data and the desire for commercial entities to obtain them. Moreover, databases of personal information are concurrently associated with junk email containing advertisements[51] and phishing[52].

Solove states that "Internet is rapidly becoming the hub of the personal information market"[53]. Indeed, a database of personal and sensitive information helps commercial entities to know about consumers preferences or sexual orientation and that "authorizes" them to send to consumers emails and pop-up

[45] Ibid.
[46] Lloyd I, n 12 above, at 46.
[47] De Cock Buning, n 22 above, at 310.
[48] Edwards, n 7 above, at 227.
[49] Ibid.
[50] Edwards n 7 above at 229.
[51] Ibid .
[52] Lynch, n 23 above at 262.
[53] Solove J, "*Privacy and power: Computer Databases and Metaphors for Information Privacy*" 53 Stamford Law Review, 2001, at 1409.

advertisements in order to seduce us and buy their products. To make matters worse, pop-up advertisements can reveal consumers' preferences to a third person who by chance used the consumer's computer for web browsing. However this threat definitely can discourage a consumer from net-shopping. A survey by the Department of trade and industry (DTI) found that 30% of those questioned would not shop on the internet and 20% also cited fears about disclosing personal information; moreover a third of those questioned had bought from abroad and over the half of them stated that they would never again do so[54].

The problem of the infringement of consumers' privacy becomes bigger when business holding personal information may disclose it to third parties either deliberately or accidentally[55]. Moreover, the information sharing between companies or agencies can cause many problems for instance health insurers might learn that the insured is checking out AIDS sites[56]. Cookies make things easier for business in order to collect information because there are computer storage programs and record all the online activities of the users[57]. The cookie can read stored information and analyze the viewing habits of the visitor; moreover they can spy and follow a user from website to website[58]. Privacy is invaded by reviling one's hidden world, by surveillance and by disclosure of concealed information[59]. Can consumers really be left alone when they are on-line? David Brin states that is far too late to prevent the invasion of databases[60].

Solove observes that privacy law consists of a mosaic of various types of law: tort law, constitutional law, property law and contract law[61]however is not just that, it has to be a global action from all countries as well thus international cooperation and international treaties have a great role to play. He argues that a solution is a set of laws and rights that will govern our relationship with public

[54] DTI surveys available at: http://www.dti.gov.uk/ccp/topics1/pdf1/ecomm2.pdf.
[55] Edwards, n 7 above, at 231.
[56] Edwards, n 7 above, at 232.
[57] Chissick M, Kelman A, "*Electronic commerce, law and practice*", (3rd edn, 2002, Sweet and Maxwell), at 221.
[58] Ibid.
[59] Solove, n 53 above, at 1398.
[60] Brin D, "*the transparent society: will technology force us to choose between privacy and freedom?*" 8 Stamford law review 1998 at 25.
[61] Solove, n 53 above, at 1430.

and private bureaucracy and the enforcement of prior consent (opt-in instead of opt-out). [62]However the European Telecom-privacy directive provides for the opt-in.

Protection of private life is a subject of different international and European treaties such as Article 8 of the European Convention of Human rights and fundamental freedoms, Article 12 of the Universal Declaration of Human rights and of Article 17 of the International Convention on Civil and political rights and the Convention 108 for the protection of individuals with regard to automatic processing of personal data.[63] However, in the above mentioned regulatory regime there is not any specific provision for data taken from children; children can easily give away "sensitive" data because of unawareness[64]. Law should deal with that issue and introduce specific legislation equivalent to the US Children's on-line privacy protection Act.

On a European level there is the directive 95/46 concerning the processing of personal data and the protection of privacy but the crowing problem of intrusion in our privacy obliged legislators to go further than the existing regime and regulate adequately the consumers' right to privacy[65]. Thus it was adopted the 97/66 directive dealing with processing of personal data and the protection of privacy in the telecommunications sector.

The E.U was concerned with the problem of privacy recognised that legal, regulatory and technical provisions should be harmonized in order to avoid such obstacles to the internal market[66]. Thus it adopted the 2002/58 directive and repealed the 97/66 directive[67], which is more sophisticated and improved compared to the directive 97/66(the telecommunication directive) especially articles 5 and 13 that have direct impact on e-commerce. However, privacy protection is a global issue and the only satisfactory way of combating the

[62] Solove, n 53 above at1456.
[63] Lodder, n 35 above, at 119.
[64] De cock Buning, n 22 above, at 312
[65] EU Directive 2002/58/EC, recitals 5-7.
[66] Recital 8 of the Directive 2002/58 EC.
[67] Article 19 of the 2002/58 EC.

problem is by international solutions but not just implementation of legal rules but it has to be created effective enforcement mechanisms[68].

The privacy Directive 95/46 aims to protect the privacy of individuals and the free flow of personal data between member states[69].It defines personal data with the test of the possibility to identify the person behind the information[70]. However, there are problems not dealt with such as emails when the identity of the user can be identified and with IP-numbers because of the possibility for an ISP to link the number to a certain computer and therewith a person[71], moreover when connecting to the internet via telephone line (dial-up) the ISP can indirect identify the user[72].

The 2002/58 Directive in Article 5 deals with the confidentiality of the communications. It deals especially with cookies and spam and requires that cookies may only be set if the consumer "is supplied with clear and comprehensive information" about the process of information. However, this provision raises many issues on effectiveness and enforcement. Moreover, Article 13(2,3) allows the use of electronic details from natural and legal persons but in order to do that they have to give the opportunity to customers to object free of charge and in an easy manner.

The European legal regime it is not enough to deal with the protection of privacy and consequently there is a lack of consumers' confidence in e-commerce. European legislators did not give enough protection to consumers and someone could say that they are in favour of commercial entities; it is self evident that the consent of users for processing their personal data after they have taken them is not a solution. The surveillance of the consumers on-line would only stop if the law is drastic instead of describing the problem and establishing "a code of practice". Thus flexible criminal law sanctions should be established in order to

[68] De cock Buning, n 22 above, at 312.
[69] Article 1 of 95/46 EC Directive.
[70] Recital 26 of 95/46
[71] Schaub, n 34 above, at100
[72] Bergkamp L, and Dhont J, "*Data protection in Europe and the Internet: An analysis of the European's community's privacy Legislation in the context of the world wide wed"*, 7 the EDI law Review 2000 at 75.

minimize the growing problem. Moreover, it should be given the right to consumers to ask for adequate provisional orders from the court.

## Conclusion

Nowadays online shopping provides to consumers many advantages; they can compare prices, they can get a better deal, they can save time and they have access to all jurisdictions. However there are disadvantages that discourage them from doing so; the risk of fraud and the intrusion to their privacy undermine the above advantages. The law has to deal with the new problems that internet introduced and regulate it adequately especially in favour of the weak parties, the consumers.

Fraud is an exciting risk and because of the not enough and cooperated legal regime between countries allows hackers and phishers to act. Consumers having in mind that they might shop from a non-existence company, or that someone might get their credit card number and spend their money or that their order will not be adequately executed or that they might receive damaged or defective products are quite hesitant whether they should shop on-line or go to their local shop. The law has to go further from the existing regime and create confidence to consumers equal to the off-line environment. Thus, it should abolish the pre-payment regime and enforce a different approach for payment, enforce criminal laws with lower level of intention against hackers, phishers, internet service providers, employees in commercial entities that have access to personal information and credit card numbers. The chargeback system and zero liability are very practical solutions and they should be enforced by law, moreover the sellers should be obliged to comply with high security standards such as SSC, and furthermore the creation of cyber courts and on-line dispute resolutions are necessary.

Consumers apart from fraud they are discouraged from the intrusion to their privacy. The collection, processing of their personal data creates personal profiles which results to receiving daily pop-ups and emails. Moreover it results undesired advertisement because they know the user's preferences. Furthermore it gives information about consumers to thirds without consumers' authorization.

Data storage and surveillance are a threat to consumers and there is a need for the protection of the human right of privacy. David Brin[73] stated that is too late to prevent the invasion of databases; however the law can go further and impose criminal liability and orders for detention of such databases. Moreover, it should be enforced that consent on the processing of data should be given in writing in the form of an e-mail.

Surveys prove that the existing legal regime is not enough in order to give confidence to consumers. Few of the weak points of the current legal system have been discussed in this paper but it needs political decision and international cooperation to deal with them. The European Union has adopted various Directives and an International Convention on Cyber-crimes. However the Directives as noted above they have some weak points that need to be clarified and supplement and the Convention has not been adopted by all countries. Furthermore it has to be highlighted that enforcement of the law is the main problem. Especially when the crimes are committed from other jurisdiction the cost of enforcement will normally overweigh the consumers' claim[74]. Consumers will be more encouraged to engage themselves into an on-line transaction when they will feel that the law has safeguards to protect their interests as in the offline world.

[73] Brin D, n 60 above at 25.
[74] Reed C, "*Internet Law, Text and Materials*"(2nd edn,2004, Cambridge), at 299.