

**International Association of Consumer Law/Association
Internationale de Droit de la Consommation**

Newsletter 1:2 March 2004

<i>Introduction</i> _____	2
<i>Commentaries</i> _____	4
Federal Regulation of Unsolicited Commercial E-Mail in the United States _____	4
Privacy of Medical Information: Federal Court Quashes Justice Department Subpoena for Hospital Abortion Records _____	11
Recent Developments: Consumer Credit and Insolvency _____	13
Consumer protection developments _____	15
<i>Upcoming Conferences</i> _____	16

Introduction

By Iain Ramsay, Professor of Law, Osgoode Hall Law School, York University, Toronto, Canada.

This is the second Newsletter of the Association. In this issue John Rothchild presents an appraisal of the recent US Federal law regulating unsolicited commercial e-mail (spam) in the US as well as providing comparative notes on European and Australian developments. The New York Times reported on March 11 the first suit by internet companies against spammers under the Act. James Nehf discusses an important recent federal case in the US concerning the privacy of medical records. There are also notes on recent developments in consumer credit and insolvency by Iain Ramsay and updates on European Union and Greek consumer law by Vassili Christianos.

In an earlier note to members I indicated that I attended the very successful World Congress of Consumers International in Lisbon in October 2003. One issue for our Association is the relationship that we might have with CI. For example, there may be valuable synergies from closer links. One possibility would be to hold the our International Consumer law conference in conjunction with CI. This would provide an opportunity for our members to have a broad audience for their research. There are obviously many issues that would have to be discussed before making any further moves in this direction and I would invite members to share their thoughts on this issue. You can send a message directly to IACL@yorku.ca or alternatively send a message to me that I will circulate.

I would like also to invite members to contribute to the newsletter. I will send out a reminder closer to the date of the next newsletter in the summer of 2004. We particularly welcome contributions in French as well as English.

Introduction

C'est le deuxième bulletin de l'association. Dans cette issue John Rothchild présente une évaluation de la loi fédérale récente des USA réglant le E-mail commercial non sollicité (Spam) aux USA aussi bien que fournir les notes comparatives sur des développements européens et australiens. Le New York Times ont rendu compte mars 11 que le premier costume par des compagnies d'Internet contre des inondateurs sous la Loi James Nehf discute un cas fédéral recent important aux USA au sujet de l'intimité des disques médicaux. Il y a également des notes

sur des développements récents dans le crédit à la consommation et l'insolvabilité par Iain Ramsay et des mises à jour sur l'union européenne et la loi grecque du consommateur par Vassili Christianos.

Dans une note plus tôt aux membres j'ai indiqué que j'ai assisté au congrès très réussi du CI à Lisbonne en octobre 2003. Une issue pour notre association est le rapport que nous pourrions avoir avec ci. Par exemple, il peut y avoir des synergies valables des liens plus étroits. Une possibilité devrait tenir la notre conférence internationale de loi du consommateur en même temps que ci. Ceci présenterait un moyen de nos membres d'avoir une large assistance pour leur recherche. Il y a évidemment beaucoup d'issues qui devraient être discutées avant de faire toutes les plus nouvelles démarches dans cette direction et j'inviterais des membres à partager leurs pensées sur cette question. Vous pouvez envoyer un message directement à IACL@yorku.ca ou alternativement m'envoyer un message que je circulerai.

Je voudrais également inviter des membres à contribuer au bulletin. J'enverrai un rappel plus près de la date du prochain bulletin en été de 2004. Nous faisons bon accueil en particulier à des contributions en français comme l'anglais.

Commentaries

Federal Regulation of Unsolicited Commercial E-Mail in the United States

By Professor John Rothchild, Wayne State University, USA

On January 1, 2004, the first federal law specifically regulating unsolicited commercial e-mail in the United States went into effect. The CAN-SPAM Act — an acronym for the ungainly Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 — was enacted with overwhelming support in both houses of Congress, following more than six years of unsuccessful congressional efforts to pass a spam bill.

The underlying philosophy of the Act is that unsolicited electronic mail is a legitimate channel of marketing that merits federal protection against both unscrupulous marketers, who would pollute this channel with deceptive and offensive marketing messages, and overzealous state regulators, who would close off the channel altogether. The approach of the Act discloses five primary components: (1) prohibition of deceptive and offensive conduct; (2) requiring marketers to present a modest degree of accountability and responsiveness to their target audience; (3) preemption of state laws that interfere with legitimate marketers' use of unsolicited e-mail communications; (4) an enforcement scheme; and (5) further study of several more-controversial regulatory measures.

1. Prohibition of deceptive and offensive conduct. The Act makes unlawful certain conduct in connection with the sending of a “commercial electronic mail message,” which is defined as an e-mail message “the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.” 15 U.S.C. § 7702(2).

Some types of prohibited conduct are subject to criminal penalties, both fines and imprisonment. Conduct made criminal includes knowingly:

- Transmitting “multiple” commercial electronic mail messages from or through a third-party's computer without that party's authorization. 18 U.S.C. § 1037(a)(1),

(2). (“Multiple” is defined as more than 100 messages a day, 1,000 messages a month, or 10,000 messages a year. Id . § 1037(d)(3).) This prohibition is aimed at the practice, common among spammers, of disguising the origin of their messages by commandeering an innocent third-party's computer or by sending or “relaying” their messages through an unsecured third-party server.

- Including false “header information” in multiple commercial messages. Id . § 1037(a)(3). “Header information” includes the routing information, showing the source and destination of the message and the route it followed, that accompanies an e-mail message. As defined in the Act, it also includes the “From:” line. § 7702(8). This provision is aimed at the common practice of forging header information to disguise the origin of the messages.
- Registering five or more e-mail accounts, or two or more domain names, using false identity information, and using any such account or domain name to transmit multiple commercial messages. 18 U.S.C. § 1037(a)(4).
- Falsely representing oneself as the registrant of five or more IP addresses, and using them to transmit multiple commercial messages. Id . § 1037(a)(5).
- Sending a message with sexually oriented content that fails to contain a particular notice (to be prescribed by the Federal Trade Commission) in the subject line, or that displays any sexually oriented material to the recipient without his taking any steps to view it. § 7704(d). This prohibition is designed to allow recipients to set their e-mail clients to identify and dispose of such messages automatically, and to prevent children from inadvertently being exposed to inappropriate material.

Other types of prohibited conduct are subject to civil enforcement, including the following:

- Sending a commercial message, or a “transactional or relationship message,” with false or misleading header information. This practice is defined to include sending a message with accurate header information from an e-mail address that was obtained by means of false pretenses, and using header information that misidentifies the computer from which the message was sent. § 7704(a)(1).
- Sending a commercial message with a deceptive subject line. § 7704(a)(2).
- Allowing one's goods or services to be promoted via e-mail containing false header information, if the seller took no reasonable steps to prevent the sending of the e-mail, or to detect it and report it to the FTC. § 7705(a).

- The Act creates liability for rendering certain types of assistance to those who send commercial e-mail in violation of the Act. Unlawful assistance includes:
 - Providing a list of e-mail addresses to a sender, with knowledge that the addresses were obtained through forbidden harvesting or dictionary attacks (described below in paragraph 4). § 7704(b)(1)(A).
 - Providing goods or services (including, for example, website hosting or office space) to a business that promotes its products using commercial messages with false header information, if the provider has actual knowledge that the products are being so promoted and receives an economic benefit from that promotion. § 7705(b)(2).

2. Sender accountability and responsiveness. Several provisions of the Act are designed to assure that the sender of a commercial electronic mail message will be identifiable as such, and to require senders to be responsive to a recipient's expressed preference not to receive additional messages from that sender:

- Each commercial message must include an online mechanism, such as an e-mail link, allowing the recipient to indicate that she does not wish to receive future commercial messages from the same sender, and the sender must honor such opt-out requests. In addition, the sender may not transfer to anyone else the e-mail addresses of those who have exercised their opt-out rights. § 7704(a)(3), (4). This prohibition responds to the spammer's practice of interpreting an opt-out request as a verification that the e-mail address of the requester is an active address, and including that address on a list to be used by other spammers.
- Each commercial message must include the sender's physical postal address. § 7704(a)(5)(A)(iii). Holding senders of commercial e-mail messages accountable for their actions requires knowing where they are, and spammers commonly do not voluntarily disclose their geographical location.

3. Preemption of state laws. In keeping with its philosophy that unsolicited commercial e-mail is an appropriate method for marketing goods and services, the Act preempts any state law “that expressly regulates the use of electronic mail to send commercial messages.” However, the Act preserves state law to the extent it prohibits falsity or deception in connection with commercial e-mail. It also preserves state law that is not specifically applicable to e-mail. Thus, state law of

trespass to chattels, contract, and tort, and laws prohibiting fraud or computer crime, remain available. § 7707(b).

4. Enforcement. The Act may be enforced by the Federal Trade Commission (and certain other federal agencies with respect to violators that are outside the FTC's jurisdiction), the state attorneys general acting as *parens patriae*, and Internet service providers that are harmed by violations. The federal agencies enforce the Act as though the unlawful conduct were a violation of the Federal Trade Commission Act or an FTC trade regulation rule. § 7706(a)-(d).

In actions brought by states or ISPs, actual damages are available, as are injunctions, statutory damages, and attorney's fees. Statutory damages may reach \$2 million, and may be tripled in the case of willful violations or those involving defined aggravating factors. § 7706(f)(3)(C), (g)(3)(C). The aggravating factors include:

- Knowingly sending a commercial message to an e-mail address that was harvested, using a software bot or other automated means, from a website that displays a notice stating that addresses on the site may not be used for such purposes; or to an address created using a “dictionary attack,” which consists of generating e-mail addresses by combining characters more-or-less randomly. § 7704(b)(1)(A).
- Using automated means to open multiple e-mail accounts that are used to send unlawful spam. § 7704(b)(2).
- Relaying unlawful spam through a third-party computer. § 7704(b)(3).

5. Further study of additional measure. The Act directs the Federal Trade Commission to study and report on several additional issues:

- Within six months after enactment, the FTC must submit a report that “sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail Registry.” Nine months after enactment, the Commission is permitted, but not required, to implement its plan. § 7708.
- Within nine months after enactment, the FTC must submit a plan for rewarding those who provide information leading to the FTC's collection of a civil penalty against a violator. The plan must provide for such informants to receive at least 20 percent of the total civil penalty collected. § 7710(1).

- Within 18 months after enactment, the FTC must submit a plan for requiring each commercial e-mail message to contain an identifier in the subject line, such as “ADV,” that allows the message to be filtered automatically by mail client software. In the alternative, the FTC may submit “an explanation of any concerns the Commission has that cause the Commission to recommend against the plan.” § 7710(2).

Observations:

A national Do-Not-E-mail list

The Do-Not-E-Mail Registry that the FTC is directed to report upon is inspired by the telemarketing Do-Not-Call Registry. A consumer who does not wish to receive unsolicited calls from commercial telemarketers may place her telephone number on the Registry. A commercial telemarketer who makes a call to a number on the Registry is subject to substantial penalties. See 16 C.F.R. § 310.4(b)(1)(iii)(B). The FTC was strongly supportive of the telemarketing Do-Not-Call list, and indeed promulgated it by regulation in 2003. The anti-telemarketing list has also proved wildly popular with the public: over 50 million telephone numbers were placed on it during the first few months of its operation. But the FTC's Chairman, Timothy Muris, has spoken just as strongly against an analogous Do-Not-E-Mail Registry. Muris observes that unlike telemarketers, most spammers do not respect the laws, and that spammers can easily conceal their identities and operate from outside the U.S. borders, making enforcement problematic.

Preemption of state laws

Starting in 1997, state legislatures began enacting laws regulating the sending of spam to or from the state. By the end of 2003, some 36 states had enacted laws addressing spam. Most of these laws did not ban spam, but regulated it in various ways. Two of the states, however, effectively banned unsolicited commercial messages by imposing an opt-in requirement. Delaware's law, enacted in 1999, contained some odd wording, and did not seem to trouble e-mail marketers. But California's statute, enacted in September 2003, and scheduled to go into effect January 1, 2004, was more worrisome to marketers. The California law makes it illegal to “[i] nitiate or advertise in an unsolicited commercial e-mail advertisement from California [or] in an unsolicited commercial e-mail advertisement to a California electronic mail address.” Cal. Bus. & Prof. Code § 17529.2. An e-mail message is unsolicited unless the recipient has expressly consented to receive it, or the recipient has a pre-existing business relationship with the sender. Id . §

17529.1(o). The impending effective date of the California statute gave added impetus to those who supported enacting a federal law that would preempt state laws.

Requiring an identifier in the subject line

Many of the state spam laws that the Act preempts required senders of commercial e-mail messages to include a specified string of characters in the subject line of each message. Typical is a provision from the Maine law, which states:

All unsolicited commercial e-mail must contain:

A. In the subject line:

- (1) the first 4 characters as follows: “ADV:”; and
- (2) if the unsolicited commercial e-mail contains information about material that may be viewed only by a person at least 18 years of age, the first 8 characters as follows: “ADV:ADLT” 10 M.R.S.A. § 1497(3).

The idea behind these provisions is that they allow the recipient to control her in-box by setting her mail reader automatically to filter messages containing the prescribed string of characters in the subject line (in this case, “ADV:” or “ADV:ADLT”). The filtered message may be sent directly to the trash folder—or, if the recipient is a big fan of spam e-mail, to a folder that is accorded heightened priority. The CAN-SPAM Act requires messages containing sexually oriented material to be so labeled, but does not require any label for other types of commercial messages. Instead, it requires the FTC to report on the possibility of adding such a requirement; and it forbids the FTC to promulgate, by regulation, a requirement that messages be labeled in such a way as to permit easy automated filtering. § 7711(b).

Wireless spam

The Act contains a special provision dealing with commercial e-mail messages that are sent to mobile telephones and other wireless devices. It requires the Federal Communications Commission to promulgate rules protecting consumers against unwanted e-mail messages sent to their mobile phones. In particular, the rules must provide mobile phone subscribers with the ability to avoid receiving messages from a sender “unless the subscriber has provided express prior authorization to the sender.” § 7712(b)(1). This is a regime of opt-in control — a subscriber who so chooses will not receive any spam to her telephone unless she affirmatively requests it — and is accordingly more protective than the opt-out regime the Act establishes for spam sent to a

computer — a marketer is free to send unsolicited advertisements unless and until the consumer affirmatively directs it to stop.

Comparative note

Spam regulations in several foreign jurisdictions are far more restrictive of spam than is the CAN-SPAM Act. A European Union Directive generally bans commercial e-mail, in the absence of prior consent or a pre-existing business relationship. See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 O.J. (L 201) 37.

In December 2003, the Australian Parliament enacted a law that makes most commercial e-mail unlawful. There are exceptions for certain messages from government bodies, political parties, religious and charitable organizations, and educational institutions, for purely factual messages, and for messages that the recipient has consented to receive. See [Spam Act 2003, No. 129](#).

Privacy of Medical Information: Federal Court Quashes Justice Department Subpoena for Hospital Abortion Records

By James P. Nehf Professor of Law and Cleon H. Foust Fellow, Indiana University School of Law and Visiting Professor, University of Georgia School of Law

A recent decision of a federal district court in Illinois discussed the relationship between the patient privacy rules under the recent Health Insurance Portability and Accountability Act (HIPAA) and conflicting state privacy laws. In a noteworthy opinion that attracted national attention, the court in *National Abortion Federation v. Ashcroft*, 2004 U.S. Dist. Lexis 1701, held that the more stringent state privacy protections should prevail over the weaker federal law.

In November 2003, the National Abortion Federation and several physicians brought a highly-publicized legal action challenging the constitutionality of the controversial Partial Birth Abortion Ban Act of 2003, 18 U.S.C. § 1531 (PBABA), a law that prohibits certain late-term abortion procedures regardless of the medical reasons for the procedure. During the course of litigation, one of the plaintiffs, Dr. Cassing Hammond, declared that he performed late-term abortions only for the protection of his patients' health. In an effort to discredit Dr. Hammond, the Justice Department subpoenaed records from Northwestern Memorial Hospital in Chicago (where Dr. Hammond performed his procedures), seeking to establish that the abortions were not medically necessary. The subpoena allowed the hospital to redact the patient's names and other identifying information from the records, but the patients' medical histories and other diagnostic information had to be turned over.

In a February 5 decision, Judge Charles P. Kocoras, Chief Judge of Illinois' northern district, quashed the subpoena, concluding that the privacy laws of Illinois were not preempted by the HIPAA rules, and release of the records was prohibited by the more stringent state privacy laws.

In 1996, Congress enacted HIPAA to ensure that individuals could maintain employer-provided health insurance if they lost a job or moved to a different employer. The law also set a relatively high level of privacy protection for medical records in general. HIPAA had no immediate effect when enacted, but the statute called upon the Department of Health and Human Services (HHS) to issue regulations dealing with the privacy issue. The HHS rule took years to finalize and became effective in April 2003. It governs the use and dissemination of health

information generally and applies to health plans, health care clearinghouses, doctors, hospitals, and other health care providers.

Recognizing the sensitivity of health-related information, the complex HHS rule provides that in most situations covered entities must obtain patient consent before using or disclosing health information when they carry out treatment, payment, or health care operations. However, a covered entity may disclose information without patient consent in several circumstances, including in response to a court order issued in the course of legal proceedings. The Justice Department invoked this exception in seeking to enforce the subpoena against the hospital.

Significantly, the HIPAA rule did not preempt state privacy laws that are “more stringent” than HIPAA's requirements. 45 C.F.R. § 160.203(b). The Illinois Code of Civil Procedure is one such law. It provides that “no physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character” unless one of eleven enumerated conditions exists. 735 ILCS 5/8-802. Illinois courts had previously held that the Illinois law protected medical information in the possession of a hospital, even in response to a subpoena and even when patient names were redacted. *People v. Manos*, 761 N.E.2d 208 (Ill. App. 2001). Since the Justice Department did not claim that any of the eleven enumerated exceptions applied, Illinois law (as interpreted by state courts) protected the abortion records.

The Justice Department argued that the Illinois law was trumped by the Supremacy Clause of the United States Constitution, U.S. Const. Art. VI, cl. 2. This would ordinarily be a compelling argument, but Judge Kocoras noted that the Illinois privacy protections were activated only through HIPAA's anti-preemption provision. This was not a case of state law trumping federal law, but rather a case of one federal law (HIPAA and its anti-preemption provision) displacing another (the PBABA).

The case is significant as one of the first applications of the HIPAA anti-preemption provision. The court read the provision broadly, incorporating case law from lower courts in Illinois to expand the scope of the Illinois statute and protect patient records that would not be protected under federal law. It opens the door for states to enact more stringent patient privacy laws than the federal law recognizes. It also lends further support to the view that strong privacy laws in the United States (indeed strong consumer laws generally) are emanating more frequently from the individual states rather than the federal government.

Recent Developments: Consumer Credit and Insolvency

By Iain Ramsay, Professor, Osgoode Hall Law School, York University, Toronto, Canada

The UK government has published a White Paper on the reform of the law of consumer credit. The White Paper should also be viewed in the light of continuing concerns about over-indebtedness in the UK and questions raised about the role of credit cards in contributing to this phenomenon. The recent report of the [Treasury Select Committee on the Transparency of Credit Card Charges](#) was critical of a number of credit market practices and included recommendations for greater transparency and more responsible lending practices. North American readers will find the report of interest since many of the marketing practices (automatic raising of credit limits, low interest introductory offers, credit card cheques, reductions in minimum repayments) originated in the US. The hearings by the Select Committee included also the unfortunate admission by Matthew Barrett, Chairman of Barclay's Bank that "[I do not borrow on credit cards: it is too expensive](#)", as well as the statutory requirement of a story that a [gold credit card offer had been sent to a dog](#). Among the Committee's recommendations was one based on the California model that would require credit card companies to indicate on monthly statements the time needed to repay a balance where an individual pays only the minimum amount. The discussion of credit and over-indebtedness should also be related to the recent reforms to personal insolvency in England and Wales that will make bankruptcy a more attractive option for overindebted individuals by reducing the discharge period to one year. Indeed in some cases a discharge may be available for a first time bankrupt in three or four months.

There is also concern with growing numbers of overindebted families in France and [recent legislative changes](#) to the procedures for addressing overindebtedness recognise explicitly the possibility of a discharge of debts and a fresh start, "un nouveau depart", for an individual debtor. For an overview and evaluation of the procedure see N. Cote, "Le Nouveau Dispositif de Traitement du Surendettement des Particuliers" Titre III de la loi no.2003-710 du 1er aout JCP G 2003, 1,175,19 November, 2003 (and see Le Monde 10.02.04). If it is determined that the situation of a debtor is "irremédiablement compromise" characterised by "l'impossibilité manifeste" of treatment short of insolvency, then an individual may be discharged from almost all her debts after 12 months and liquidation of assets (subject to certain exemptions). A note of the procedure will be recorded on the national credit bureau for a period of eight years.

Given the wide gulf that has historically existed between "Anglo-Saxon" jurisdictions and Continental European laws in their willingness to permit an individual consumer to discharge her debts in bankruptcy, the French move towards recognising a discharge is intriguing and the legislative history of the recent reforms refers to existing bankruptcy laws in the US, England and Wales, and Denmark. However, it is dangerous to suggest that there is a "convergence" of approaches in Europe to problems of overindebtedness. There remain significant differences in practical and ideological approaches to the treatment of over-indebtedness in Europe (see Nieimi-Kiesiläinen). The new French law is contained within legislation addressing urban renewal, and is partly justified as combating social exclusion caused by overindebtedness. In contrast the recent English personal insolvency reforms are nested within the Labour government's flagship Enterprise Act, intended to stimulate entrepreneurialism in the UK by reducing fear of the consequences of failure by individuals engaged in business. Since consumers, as individuals, are included within the scope of the Act, they benefit through the sidewind of this legislation.

Finally, the [European Consumer Credit Directive](#) has been severely criticised in the [European Parliament](#) (see [amended proposal by rapporteur](#) of Committee on Legal Affairs and the Internal Market European Parliament) and it is not clear what will be its ultimate future. In the US, the proposed reforms to consumer bankruptcy that would make it more difficult for consumers to access bankruptcy relief continue to stall. In Asia Consumers International has instituted a project on [regulation of consumer credit](#) and is holding a conference on the adequacy of consumer credit regulation in Asia.

Consumer protection developments

By Professor Vassili Christianos, University of Athens

European legislation

A new Regulation (261/2004) has been issued on 17 th December 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding, and of cancellation or long delay of flights, and repealing Regulation No 295/91 (OJ 2004 L46/1). The new Regulation seeks to improve quality of service of airlines provided to passengers. It raises the standards of consumer protection set by Regulation No 295/91 and expands consumer protection. While the protection of Regulation 295/91 was restricted to cases of denied boarding, the new Regulation applies also in case of delays and cancellation of flights. The protection applies not only to scheduled flights as it was provided by Regulation 295/91, but also to non-scheduled flights, including those forming part of package tours. The Regulation shall apply to passengers departing from an airport located in the territory of a Member State, or an airport located in a third country to an airport situated within the EU. In addition, Member States shall ensure and supervise general compliance by their air carriers with this Regulation and designate an appropriate body to carry out such enforcement tasks. The Regulation enters into force the 17th February 2005.

Greek case law

The Three Member Administrative Court of Athens has recognised that the Supervisory Authority of the Financial Markets is liable in damages vis-à-vis the investor as consumer of financial services, when it fails to adequately supervise investment services providers (judgment 15526/2003). This is the first judgment in Greece and, to my knowledge, the third judgment in Europe that has recognised a right to consumers for inadequate supervision by the Financial Supervision Authorities (see for France case KERCHICHIAN , Cour Administrative d ' Appel de Paris , 25.1.2000, Kechichian , Req 93 PA 01250 – Conseil d ' Etat , 30.11.2001 and for Italy case CONSOB , Italian Corte di Cassazione, sez. I civile- sentenza 3 marzo 2001 n. 3132). For a thorough analysis, see G. ALPA, “The harmonisation of the EC law of Financial Markets in the perspective of Consumer Protection,” Paper presented at IACL Conference in Athens, April 2003.

Upcoming Conferences

The following is a note from Christian Twigg-Flesner

SLS Annual Conference 2004 - University of Sheffield Consumer Law Section - Call for Papers

Dear colleagues,

The UK-based Society for Legal Scholars will hold its annual conference at the University of Sheffield this autumn (13-16 September 2004). Further details can be accessed via www.legalscholars.ac.uk . I am e-mailing in my capacity as Convenor for the Consumer Law Section with a call for papers. If you would like to give a paper at the consumer law section meeting at this year's conference, I'd be grateful if you could contact me by e-mail (christian.twigg-flesner@sheffield.ac.uk) with a short abstract of your proposed paper. It would be helpful if I could have this by the end of March.

There is no particular theme for the conference and I am therefore happy to consider papers on any aspect of consumer law. Having said this, I would, in particular, welcome papers which have a "cross-over" theme to them, i.e., papers which might consider the interaction between consumer law and other areas of law.

I should point out that speakers are required to register and pay for the conference in the normal way, and that they are also responsible for making their own travel arrangements. Further details are available on the website above.

I look forward to hearing from you.

Dr Christian Twigg-Flesner
SLS Consumer Law Section Convenor

=====

Dr Christian Twigg-Flesner
Lecturer in Commercial and Company Law
Department of Law, University of Sheffield
Crookesmoor Building, Conduit Road
Sheffield S10 1FL, United Kingdom
E-mail: Christian.Twigg-Flesner@sheffield.ac.uk
Tel.: 0114 - 2226827
<http://www.shef.ac.uk/law/staffd/twiggflesner.htm>

Consumers International Asia Pacific Office is organising the Asian Conference on the Regulation of Consumer Credit from 29-30 March 2004 in Selangor Darul Ehsan, Malaysia.

The conference will review problems faced in consumer credit transactions in Asian countries and determine the extent to which the existing laws governing credit are adequate. The specific objectives are to:

increase capacity of consumer organisations and government policy makers to understand consumer protection issues relating to consumer credit transactions;

propose reforms in the area of consumer credit and examine the viability of using guidelines/policies of other regions as a model;

raise the standard of consumer protection in credit transactions in Asian countries; and

establish greater links and exchange between Asian consumer organisations and government policy makers on consumer credit issues.

This conference will bring together representatives from consumer organisations, associations of credit providers, government policy makers researchers, and academics to discuss appropriate policy changes and regulatory measures needed to protect consumers in credit transactions.

Please direct all enquiries to Ms. Susheela Nair at susheela@ciroap.org (Tel: 603 7726 1599 Fax: 603 7726 8599).

Kindly visit the conference website at <http://www.ciroap.org/apcl/credit/conf> for latest conference information.

Contact Details: Susheela Nair

603-77261599

603-77268599

susheela@ciroap.org

Teaching Consumer Law May 21-22 University of Houston Law Center.

This year's conference will have a heavy international component. Further details contact Professor Richard Alderman at Alderman@uh.edu.