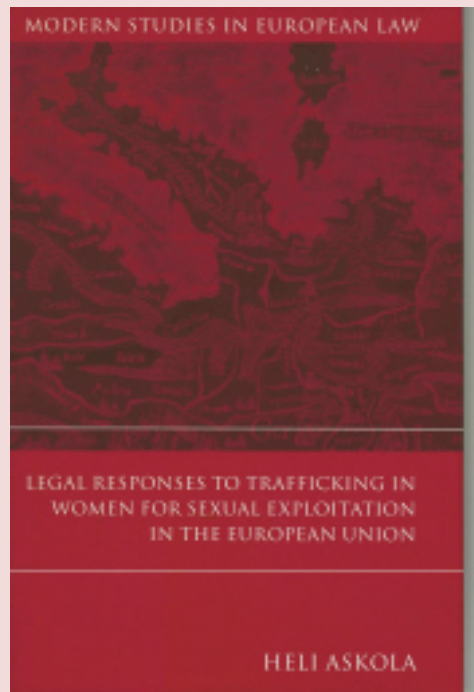


BOOK REVIEWS BY SALLY RAMAGE

Legal Responses to Trafficking in Women for Sexual Exploitation in the European Union



Edition: 1st

Author: Heli Askola

ISBN: 1-84113-650-6 / 9781841136509

Cover: Hardback

Publishers: Hart Publishing

Price £35.00

Publication Date: March 2007

Publisher's Title Information

The phenomenon of trafficking in women for sexual exploitation, which in the last decade has changed from a marginal 'non-issue' to a legitimate concern in many parts of the world, has become familiar through newspaper coverage, and now, finally, legislators and law enforcement agencies have begun to act. In Europe many EU Member States now have (or are developing) at least some sort of anti-trafficking policies (with some of them in the forefront of global anti-trafficking efforts). Moreover, the EU itself has become markedly more active with regard to curbing trafficking in human beings, as part of its migration control and police and judicial co-operation functions.

However, even co-ordinated efforts such as those being worked on by the EU tend to produce only short-term 'cures' to a problem that is in truth global and structural in nature and which cannot be eradicated - or necessarily even significantly reduced - through policing and migration control measures alone. Too often there is little debate on broader measures which might be targeted to address the 'root causes' of trafficking, such as poverty, under-development, general lack of economic and migration opportunities and, above all, gender inequality.

Against this background, this book deals with present efforts to control trafficking in women for sexual exploitation. In doing so it examines claims that what is needed effectively to prevent and tackle trafficking is a 'comprehensive' approach, and at the very least one that is far more wide-ranging and coherent than what exists today, and also analyses the assertion that destination countries, and more specifically Member States of the EU, could and perhaps should, take more action against trafficking through regional co-operation, particularly in the framework of the EU, rather than as individual Member States.

The book will be of interest to a wide range of scholars in EU law, human rights, comparative law, sociology, feminist theory and politics, as well as policy-makers, practitioners and NGO activists in various European countries.

The Author

Heli Askola is a Lecturer in Law at Cardiff University.

Review

This book essentially argues that sexual services by prostitutes are a commodity and in the EU should be lawful under the EU Freedom of Movement: but that it is not.

The author says, "The lack of will to engage in any debate over whether or not the Union should play a role in addressing demand for sexual services is actually a manifestation of a broader problem. To say this is not to claim that the European Union is the problem rather than the solution as far as trafficking in women for sexual exploitation is concerned; rather we have to recognise the multiple ways in which the European Union is part of the problem in order to conceive of ways of making it a part of the solution as well".

Framework Decision 2002/629/JHA, [2002] OJ L 203/1, largely reflects the UN Trafficking Protocol... Article 3 of the UN Trafficking Protocol states:" Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs."

Paragraph 2 of the EU Council Framework Decision 2002/629/JHA simply copies the UN Trafficking Protocol, Article 3(b) on consent, but the EU Council Framework Decision introduces additional provisions such as the demand for sanctions against trafficking to be effective, proportionate, minimum, and maximum penalties.

The United Nations Trafficking Protocol established the first internationally agreed definition of the crime of trafficking in humans, but this book averts itself from the criminality of trafficking. Throughout the book, the term irregular immigration is used, rather than illegal immigration. It concentrates on the “freedom” of movement and states in Chapter 3, “Freedom after all, is a central and cross-cutting feature of European integration, whereas victims of trafficking are in some ways the personification of the un-free...”, claiming that trafficking is rarely extended to address the working of the Internal Market of the European Community. Yet, earlier parts of the book state that prostitutes are not necessarily passive victims of a patriarchal society and that prostitution is not always inherently exploitative, it can also be well paid. The writer argues that expansion of sex-industries in many countries is not due to natural male urges, but as in any market, to sex-business entrepreneurs who actively create and expand the demand for an ever-widening range of ‘sexualised’ services...

In examining prostitution in EU countries, the writer admits that Sweden has criminalised prostitution whereas in the Netherlands the ban on brothels was lifted in the year 2000. The writer missed a strong point in her argument by ignoring Germany where legalisation of prostitution is being considered and, as if the UK were not a member of the EU, the writer side-lined the UK situation altogether, (in the book, *Wicked beyond Belief* by Michael Bilton, (pg 306), he wrote that, in searching for the Yorkshire Ripper who murdered prostitutes some decades ago, police details of all known men regularly visiting prostitutes in West Yorkshire and Manchester alone, revealed that 21,000 males were “punting” prostitutes in one 18-month period alone, - thereby missing a strong argument to support the thesis.

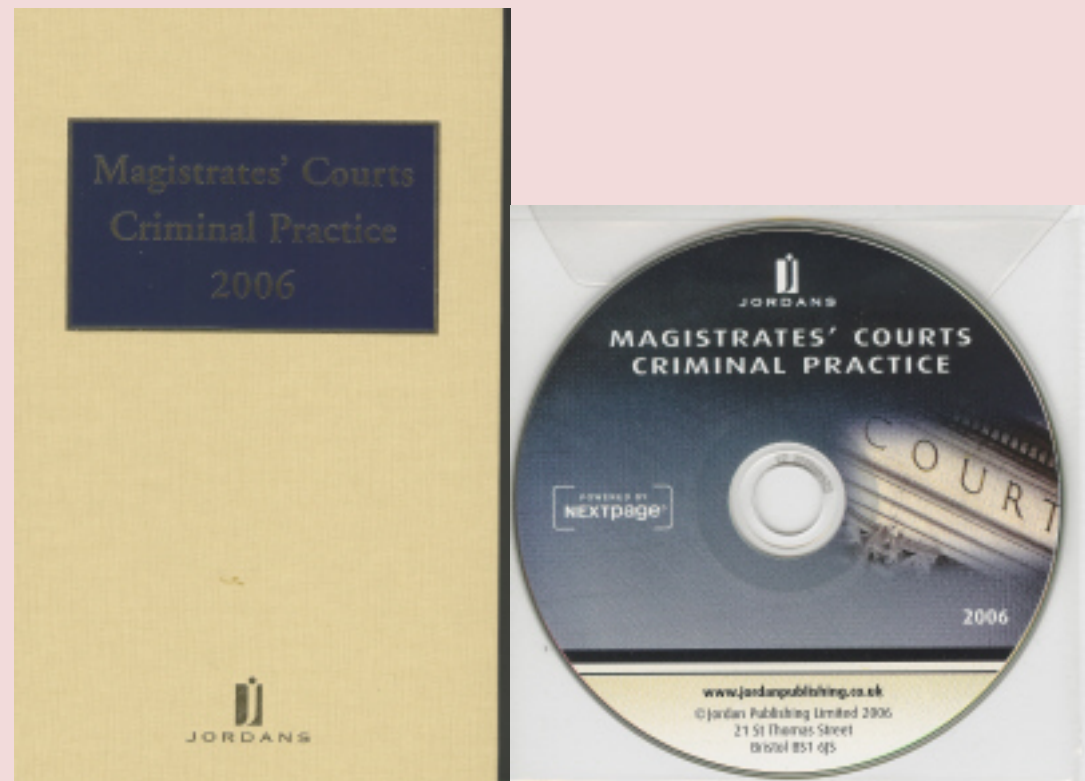
There are 900,000 to 1,000,000 trafficked prostitutes in the world, according to statistics by the US State Department. It would have been enlightening for the writer to tell us approximately how many of these are trafficked to the EU, as this would have strengthened the hypothesis that the EU should view trafficking under the Freedom of Movement of workers. The writer did however acknowledge that the service industries, especially the feminised sectors of care and domestic work, which absorb a large proportion of female migrants, are typically associated with informality and irregularity of working conditions.

I think that this academic exploration into trafficking of women for prostitution is a welcome addition to the list of scarce writings on the subject and will add to the debate.

Sally Ramage

May 2007-07-30

Magistrates' Courts Criminal Practice 2006



REVIEW of JORDAN'S MAGISTRATES COURTS CRIMINAL PRACTICE 2006

By

Sally Ramage

This book, as one of its category, uplifts the spirit. I cannot enthuse about it enough.

Firstly, the book cover is light-coloured and tactile, a similar good book cover I have not seen since Butterworth's "Clark Hall and Morrison on Children". I noticed the very sensible feature of a soft but strong book spine, necessary for a large book regularly used. It features a useful touch of including three years calendar at the front.

Jordan's Magistrates Courts Criminal Practice a good, well-designed manual. Its contents are laid out in an excellent manner in 7 parts:

Part I Procedural Guides

Part ii Elements of Offences

Part iii Statutes

Part iv Statutory Instruments

Part v Practice Directions

Part vi Codes of Procedure and guidelines

Part vii Non-prescribed Forms

The book consists of 2422 pages, the first 567 pages being the essential manual, the rest being cross-referenced materials. As to the many pages of statutes, I wonder why the method used by some publishers of including only the relevant parts of a statute, rather than the complete statute, is not used to make for a lighter book.

“Part ii. Elements of offences” is the essential star ingredient in the book. To this effect, it may benefit from being comprehensive. The elements of offences are brilliantly laid out but only tackle 82 criminal offences before the Magistrates Courts, these being affray; aggravated vehicle taking; animal cruelty; assault; breach of requirement of a Community Order; breach of an Anti-Social behaviour order; burglary; common assault; criminal damage; disorderly behaviour; drugs misuse; drugs possession; drugs supply; drugs cultivation; drunk and disorderly; evasion of Duty; failure to surrender to bail; football related offences; going equipped for theft; handling stolen goods; harassment; sexual assault; indecent photographs of children; making off without payment; obstructing a police officer; possession of a bladed weapon; possession of an offensive weapon; racially or religiously aggravated assault; racially or religiously aggravated criminal damage; racially or religiously aggravated disorderly behaviour; racially or religiously aggravated harassment; racially or religiously aggravated threatening behaviour; racially or religiously aggravated wounding; school non-attendance; social security offences; taking a vehicle without consent; theft; threatening behaviour; vehicle interference; violent disorder; wounding; careless driving; dangerous driving; driving whilst disqualified; excess alcohol and driving; failure to stop; no insurance;; alcohol/drugs unfitness for driving; refusing evidential specimen; refusing roadside breath test; driver not supplying details; licence offences; driving without lights; not notifying DVLA of change of ownership; MOT certificate not held; traffic direction offences; failing to comply with police signs; vehicle defects; vehicle loads; motorway offences; operators licences not held for goods vehicles; tachograph offences and speed limit offences.

It is obvious that this is an excellent manual for day- to- day use by criminal law practitioners.

It could become an all-encompassing reference book of its kind if there is included in the next edition, offences not included , some of which are as follows:-

Eg 1- obtaining personal information by deception. This is a criminal offence under section 55 Data Protection Act. This could carry a £5,000 maximum fine in the Magistrates Court.

Eg 2- Parenting Orders in respect of criminal conduct. A parenting order is an order which requires the parent to comply, for a period not exceeding twelve months, with requirements in the order such as to attend counselling and guidance programmes. See Anti-Social Behaviour Act 2003, sections 19 to 22.

Eg 3- Immigration offences. See Immigration and Asylum Acts 1971, 1988, 1999. Where the offence is one to which an extended time limit for prosecution applies, an information relating to the offence may be tried by a Magistrates Court if it is laid within 6 months of the commission of the offence, or if it is laid within 3 years of the commission of the offence and not more than 2 months after the date certified by a police officer above the rank of chief superintendent to be the date on which evidence sufficient to justify proceedings came to the notice of the officer of the police force to which he belongs.(Immigration Act 1971,Part 111,sections 24-28 as amended).

Eg 4- Cruelty to animals offences- see Protection of Animals Act 1911,section 3 and Protection of Animals (Amendment) Act 1954, section 1(2).

Eg 5-Offence of bird poaching. See Protection of Birds Act 1954, section 15(2).

Eg 6- The new fraud offence. See Fraud Act 2006.

Eg 6- Breaches of health and safety.

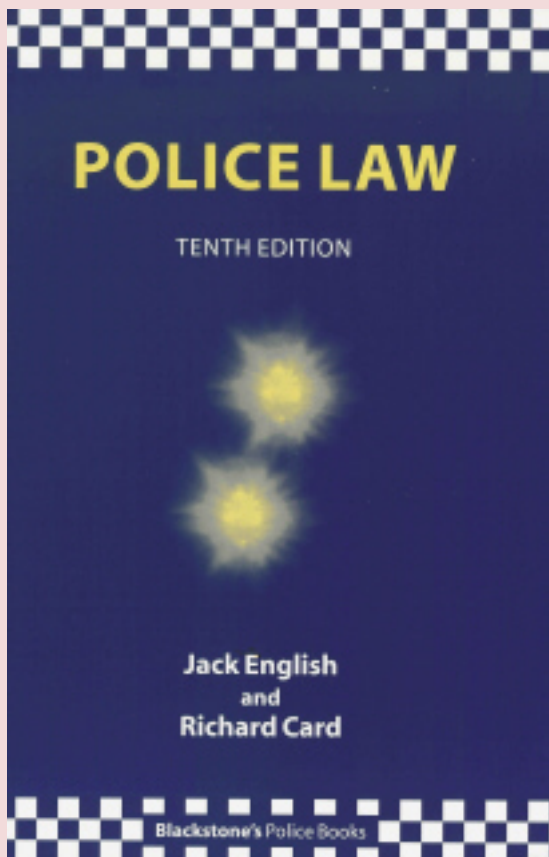
Eg, 7- Noise related regulatory offences.

Eg 8- Consumer credit offences and offences relating to advertising. An offence under the Consumer Credit Act is punishable on summary conviction by a fine not exceeding the prescribed sum and on conviction on indictment by a maximum of 2 years imprisonment or a fine or both. (Amended by the Magistrates Courts Act 1980 section 22(2)).

Jordan's Magistrates Court Criminal Practice is an excellent book in concept and design. An improved and updated new edition is awaited.

Sally Ramage

Police Law



Edition: 10th

Authors: Jack English & Richard Card

ISBN: 10: 0-19-921406-9

Publishers: Oxford University Press

Price £27.95

Publication Date: 15 March 2007

Publisher's Title Information

This well-respected and highly regarded book, now in its 10th edition, covers all areas of law and legal procedure which are of interest to police officers.

Comprehensive and easy to understand, it is suitable for any reader, even those with no formal legal training. In addition, it will be of particular assistance to all those who are studying Criminal Law for the first time. The book also provides a good source of information for members of the public who wish to refer to a legal text written in an accessible way.

Formerly known as Butterworth's Police Law, this edition has been fully updated and now includes discussion of the Serious Organised Crime and Police Act 2005 (SOCPA), the revised PACE Codes of Practice, the Gambling Act 2005, the Terrorism Act 2006, the Racial and Religious Hatred Act 2006, the Fraud Act 2006 and new traffic legislation.

This is a practical and comprehensive volume for everyday use which is now accompanied by a useful companion website, with quarterly chapter updates.

Provides comprehensive and straightforward coverage of those areas of the law and legal procedure applicable to police officers

Accessible text which assumes no prior legal knowledge

Extensive cross-referencing with clear supporting explanations

Clear and simple structure with headings breaking each chapter into manageable sections

Contains real and relevant examples covering those aspects of the Law which touch the community at large

Now accompanied by a useful companion website, with quarterly chapter updates

New to this edition

Contains all the latest case law and legislation including SOCPA 2005, the 2006 PACE Codes of Practice, the Fraud Act 2006, the Police and Justice Act 2006, and new traffic legislation.

Contents

List of Abbreviations

- 1. General principles**
- 2. Elements of criminal procedure**
- 3. Police powers**
- 4. Police questioning and the rights of suspects**
- 5. Treatment, charging and bail of detained persons**
- 6. Identification methods**
- 7. The law of evidence**

- 8. The police**
- 9. Traffic: general provisions**
- 10. Use of vehicles**
- 11. Control of vehicles**
- 12. Public service vehicles**
- 13. Goods vehicles**
- 14. Lights and vehicles**
- 15. Traffic accidents**
- 16. Driving offences**
- 17. Drinking or drug-taking and driving**
- 18. Children and young persons**
- 19. Licensed premises, licensed persons, clubs, places of entertainment and offences of drunkenness**
- 20. Betting, gaming and lotteries**
- 21. Aliens**
- 22. Animals, birds and plants**
- 23. Game laws**
- 24. Firearms**
- 25. Explosives**
- 26. Railways**
- 27. Pedlars, vagrancy and dealers**
- 28. Non-fatal offences against the person**
- 29. Disputes**
- 30. Homicide and abortion**
- 31. Public order offences other than those related to sporting events or industrial disputes**
- 32. Public order offences related to sporting events and those connected with industrial disputes**
- 33. Sexual offences, child abduction and kidnapping**

34. Offences relating to prostitution, obscenity and indecent photographs

35. Drugs

36. Theft and related offences, robbery and blackmail

37. Criminal damage

38. Burglary

39. Offences of fraud and corruption

40. Handling stolen goods and related offences

41. Forgery and counterfeiting

42. Preventive justice

REVIEW

This excellent reference book is the 'bible' of United Kingdom Police Law. It is well written. It is up-to-date and includes Control on Dogs Order 2006 (SI 2006/779); Criminal Procedure Rules 2005 (SI 2005/384); Passenger and Goods Vehicle Regulations 2006 (SI 2006/1937); the Fraud Act 2006 and the Gambling Act 2005. It has both a short and a detailed Contents List, a very useful feature.

Chapter 1 on General Principles includes a section on corporate liability, useful, especially since the Fraud Act and the Health and Safety Act address corporate liability. Offences of fraud and corruption have a dedicated chapter which also includes computer misuse. This is very apt since the Fraud Act 2006 covers the offence of 'phishing' but not some other computer offences which are being brought in by the Serious Crimes Bill 2007.

Chapter 3 includes one paragraph on 'matters subject to legal privilege' (page 101) in respect of seizure of property. My only criticism of the book that this topic was not discussed. It is a fundamental and long established principle of English law that clients should be able to communicate freely with their legal advisors, without fear that their communications will later be disclosed to their prejudice. Certain documents and discussions between professional legal advisors and their clients are therefore afforded a special level of protection from disclosure that is not generally available to communications with other professional advisers. Legal privilege covers confidential communications between a client and his professional legal advisor made for the purposes of giving, or receiving, legal advice irrespective of whether litigation is in contemplation or progress at the time. This protection applies even if the evidence is highly relevant to the issues in dispute, and it is not generally open to a court or tribunal to draw adverse inferences if privilege is claimed. Legal advice privilege is only available to the "client".

Chapter 20 deals with betting, gaming and lotteries. It was exciting to see the mention of section 41

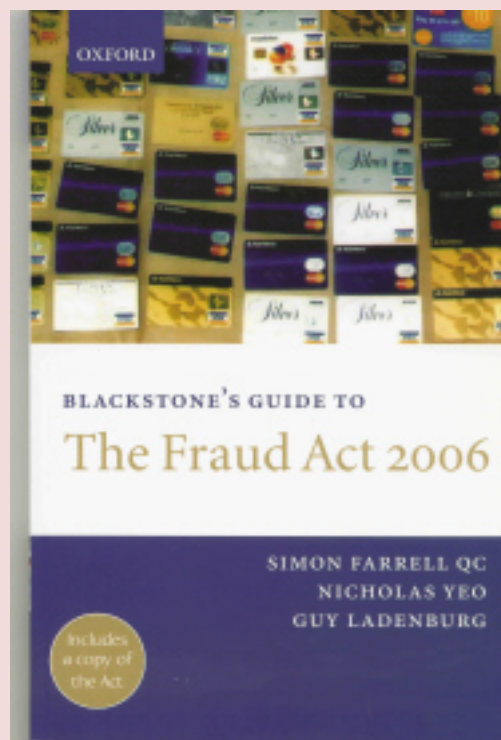
Gambling Act 2005 (page 697) which "provides that it is an offence to manufacture, supply, install or adapt, in the course of business, computer software for remote gambling except in accordance with an operating licence held for that activity." The Gambling Act 2005 will be in force in September 2007 and it will become lawful to provide remote gaming services from the UK. To coincide with this, a new gambling duty, to be called "remote gaming duty" or "RGD", will be introduced.

The book is full of gems of detailed police law. For example, the Diplomatic Privileges Act 1964 provides that ambassadors and Commonwealth High Commissioners and members of their families are immune from arrest and criminal proceedings whilst in the UK in that capacity. However, there is no immunity for a member of the family who is a national of the United Kingdom. The Metropolitan Police maintain an index of persons who are entitled to diplomatic immunity.

'Police Law' is an excellent showcase reference book of UK police law that legislators from other countries will be impressed with. All police officers need this book and all libraries throughout the United Kingdom should stock this publication. Jack English and Richard Card's 'POLICE LAW' is a true heavyweight. It is a masterly publication of top calibre standard, fluent, refreshingly clear and packed with detailed knowledge of UK police law. It is a law book one does not want to put down once one begins to read it and that makes for a winning book.

Sally Ramage

Blackstone's Guide to The Fraud Act 2006



Edition: 1st

Authors: Simon Farrell, Nicholas Yeo & Guy Ladenburg

ISBN: 0-19-929624-3

Publishers: Oxford University Press

Price £34.95

Publication Date: 29 March 2007

Publisher's Title Description

Places new offences including those of obtaining services dishonestly and of the act of possessing or making material for use in frauds, in the context of previous law

Structured in a clear and accessible way, with narrative logically following the structure of the Act

Lucid commentary on the effect of the new legislation, and guidance on its likely impact and interpretation in practice

Contains full text of the Fraud Act 2006

The Blackstone's Guide Series delivers concise and accessible books covering the latest legislative changes and amendments. Published within weeks of the Act, they offer expert commentary by leading names on the effects, extent and scope of the legislation, plus a full copy of the Act itself. They offer a cost-effective solution to key information needs and are the perfect companion for any practitioner needing to get up to speed with the latest changes.

The Fraud Act 2006 creates a new general offence of fraud with a maximum custodial sentence of ten years; replacing all previous deception offences as detailed under the Theft Acts 1968-1996. This new offence can be committed in three ways;

By false representation

By failing to disclose information

By abuse of position

The Act also creates new offences of obtaining services dishonestly, and replaces the existing 'going equipped' offence, to criminalise the act of possessing or making material for use in frauds. This new Blackstone's Guide provides the full text of the Fraud Act 2006 and extracts from related relevant legislation, together with expert narrative. The authors provide detailed and practical commentary logically following the structure of the Act, on the effect of the legislation, its probable interpretation, and its impact on the existing law of dishonesty.

Fraud is a socio-legal concept of much complexity. Fraud, like all crime, is a result of a combination of psychological and sociological factors.

Although the word "fraud" has been in use for centuries, there has never before been a legal definition of 'fraud' in English law. English offences of fraud are found in various Acts and were thus recognised by the Home Office. The Law Commission, Report No.276, Cm 5560 (2002), suggested bringing all such offences under an umbrella offence of fraud and now there is the UK Fraud Act 2006.

Section 1 of the Fraud Act creates an offence of fraud if committed by a person who breaches sections 2, 3, or 4. Section 2 deals with fraud by false representation, section 3 deals with fraud by failing to disclose information and section 4 deals with fraud by abuse of position. One example of potential complexity is the issue of fraudulent trading which is defined in the Companies Act 2006, section 993 and the Insolvency Act 1986, sections 213 and 357.

The reader is told that although the Fraud Act 2006 is a major change in the law, there are already many current legal “weapons” for prosecuting fraud that remain in UK, legislation such as: Value Added Tax Act 1994, specifically dealing with tax evasion; Criminal Justice Act 1993 - dealing with insider dealing, Theft Act 1968 - dealing with false accounting; Financial Services and Markets Act 2000 dealing with misleading market practices and Companies Act 2006 - dealing with fraudulent trading.

Chapter 3, tackling agreements to commit fraud, deals mostly with the mens rea in conspiracy and the mens rea in fraud conspiracies. Regarding mens rea of fraud offences, there is a two-way test for dishonesty- dishonesty by the ordinary standards of reasonable and honest people and where this is so, whether the defendant was aware that his conduct would be regarded as dishonest by reasonable and honest people. The accused must intend to make a gain for himself or another; to cause loss to another or to expose another to a risk of loss though gain or loss need not ensue and such gain or loss extends only to gain or loss in money or other property, property being real or personal.

As to false representation fraud as per section 2(1) of Fraud Act 2006, the actus reus is the making of a false representation. Section 2(3) Fraud Act defines a representation as any representation as to fact or law, including a representation as to the state of mind of the person making the representation or any other person. So the representation can be express or implied by conduct and therefore possible by omission, whether there is a duty to speak or not and section 2(5) provides that a representation may be regarded as made, if it is submitted on any form to any system or device designed to receive, convey or respond to communications with or without human intervention.

Section 3 Fraud Act covers silence or fraud by failing to disclose information. Moreover, “false representation” are the words used in the Fraud Act rather than misrepresentation”. The mens rea for false representation is that the defendant knew the representation was untrue or might be untrue or that it was misleading or might be misleading, with intent to gain or cause loss dishonestly.

Chapter 9 is concerned with fraud management and the future of fraud trials including the Fraud Protocol of March 2005.

Only a few books have been published on the Fraud Act 2006 and for this reason, this book by Farrell et al is compulsory reading for all criminal lawyers.

Sally Ramage

Blackstone's Police Manuals 2007



Edition: 2007

Authors: Fraser Sampson, Glen Hutton & David Johnson

ISBN: ISBN-10: 0-19-920331-8

ISBN-13: 978-0-19-920331-4

Publishers: Oxford University Press

Price £58

Publication Date: 24th August 2006

Description

Publisher's Title Information

The definitive source of information for the OSPRE® Part I Police Promotions Examinations in England and Wales - endorsed by CENTREX, this pack contains the relevant information on which candidates will be examined

New for 2007, fully updated to include the Serious Organised Crime and Police Act 2005 (SOCPA) and the revised PACE Codes of Practice

Covers new topical areas such as the Gambling Act 2005, the Terrorism Act 2006, the Racial and Religious Hatred Act 2006 and the Drugs Act 2005

Written and developed for police officers by police officers - aimed squarely at the needs of the police

Keynotes by authors break up statutory text and common law, providing clear and concise analysis of important areas

Comprehensive cross-referencing with the other Blackstone's Police Manuals for ease of reference when considering subjects across other areas

Blackstone's Police Manuals are the leading police reference texts in the UK. In addition to being the only official study guides for the police promotion examinations in England and Wales, and a recognised text for student police officers, the Manuals have quickly established themselves as the definitive reference source for all who are involved in police law and procedure. Endorsed by Centrex for OSPRE® Part 1 Promotion Examinations, the Manuals have been written in consultation with police forces across England and Wales.

Each book in this four volume pack has been revised and updated to include all recent legislative change such as the Serious Organised Crime and Police Act 2005 (SOCPA), the revised PACE Codes of Practice, the Gambling Act 2005, the Clean Neighbourhoods and Environment Act 2005, the Drugs Act 2005, the Terrorism Act 2006 and the Racial and Religious Hatred Act 2006. Also covers recent changes to road policing such as standards of driving, causing death of others, control of vehicles, speeding, licensing & obligation of drivers and drink driving.

The Manuals are widely used in the professional development of police officers in a variety of roles, making them essential reading for anyone with an interest in police and criminal law. Whether you

are a serving police officer or police trainer, a practitioner, advisor or researcher, Blackstone's Police Manuals 2007 are an essential purchase.

Readership: Primary: Student Police Officers and sergeants and inspectors promotion examinations candidates. Secondary: Qualified serving police officers and police trainers.

Previous Reviews

"The preface to the road policing manual emphasises how important road policing is in challenging dangerous, aggressive and antisocial driving as well as being of great assistance in the wider role in disrupting activities of serious and organised criminals and terrorists. It is important that officers get it right. These books will help them do just that."

Carrie Laws, Bay Advocates, Torquay, Devon, Internet Law Book Reviews, March 2006.

"Excellent and so reasonably priced... As with all the volumes of this series, the information provided is first class This is a magnificent publication for the academic or student of policing."

Police Journal August 2006.

Review of Crime Manual 2007 by Sally Ramage)

This manual is one of four volumes written for the OSPRE Police Promotion Examinations' syllabus. The manual includes the 12 topics covered in "BLACKSTONE'S POLICE Q & A-CRIME-2007", expanded into 16 parts.

"Blackstone's Police Manual -Crime" is an easy book to handle and has excellent features by way of a Table of Cases; Table of Statutes; Table of Statutory Instruments, Home Office Circulars and Codes of Practice. These tables each have an introductory section explaining the format of cases, Statutes and Statutory Instruments. The manual boasts an excellent index and paragraphing system and each paragraph has an explanatory "keynote" section below it, clarifying to the reader that the law is not exactly black and white. The manual is dedicated to the examination syllabus and covers the nuts and bolts of everyday policing. As such, it is an excellent examination manual with immaculately laid out material.

The law stated is as at 1st June 2006 and so does not address the subject of the Fraud Act 2006, which received Royal Assent in November 2006 and came into force on 15th January 2007, although the Fraud Act 2006 will not be examined until 2008. The Fraud Act 2006 repeals sections 15, 15A, 16, 20(2) and 24A of the Theft Act 1968 and sections 1 and 2 of the Theft Act 1978, replacing these with the fraud offence, a conduct offence as opposed to a result offence.

The manual mentions the Serious Organised Crime and Police Act 2005 in sections 1.12.1 and 1.13.1 and it states that SOCPA is outside the remit of this manual. However, the execution of search warrants and SOCPA section 114(8) (a) amends the Police and Criminal Evidence Act section 16(3)

so that entry and search under a warrant must be within three months from the date of issue.

Chapter 1.10, "Sexual Offences" is a most important chapter, not only for examination purposes but because very recent reports indicate the growing and continuing threat of Internet paedophiles.

Sexual Offences Act section 15 (Meeting a child Following Sexual Grooming) states that "A person aged 18 or over (A) commits an offence if

having met or communicated with another person (B) on or at least 2 occasions, he

intentionally meets B, or

travels with the intention of meeting B in any part of the world,

at the time, he intends to do anything to or in respect of B, during or after the meeting and in any part of the world, which if done will involve the commission by A of a relevant offence,

B is under 16, and

A does not reasonably believe that B is 16 or over."

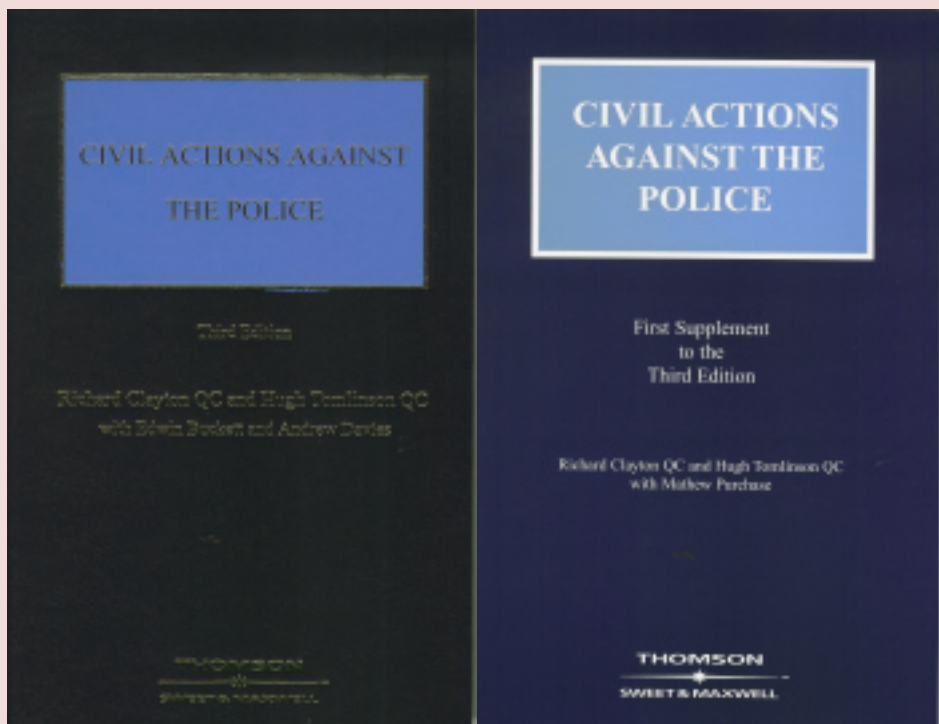
The keynote area of the section is very clear, as are all the keynote areas in the book.

Child Protection is dealt with in a separate chapter 1.11, although the keynote on the Children's Act 1989, section 49 is rather sparse and not as punchy as it could be. As an example if a father knows that his daughter is at a children's home and he assists her to run away from her carer, he will be liable under this section 49. Another example of child protection is when a school teacher, convicted of an offence involving a child, disqualified by the court from working with children, applies for a teaching post without revealing his disqualification. The school teacher is liable as soon as he applies for the job and the recruiting officer is liable as soon as he offers the job to the school teacher applicant under the Criminal Justice and Court Services Act 2000, section 35, (see 1.11. 3.1 in this volume) and from Autumn 2007, under the Safeguarding Vulnerable Groups Act 2006.

All in all, a brilliantly laid-out study volume with good keynote areas, in need of updating in the next edition.

Sally Ramage

Civil Actions against the Police



Edition: 3rd 2004, with 2005 Supplement

Authors: Richard Clayton, Hugh Tomlinson, Edwin Buckett & Andrew Davies

ISBN: 0421944706

Publishers: Sweet & Maxwell

Price £211

Publisher's Title Information

Civil Actions against the Police provides comprehensive analysis of the civil rights and remedies for police misconduct. It covers complaints against the police as well as the practice and procedure of bringing a claim.

It provides detailed explanation on the traditional tort actions that may be brought against the police as well as the developing tort of misfeasance in public office and claims in breach of confidence and data protection.

- * Covers all possible actions against the police in one place**
- * Provides detailed procedural guidance - ensuring practitioners have all the information they need when preparing a civil action**
- * Includes all the relevant documents - including PACE Codes and JSB Specimen Directions**
- * Covers damages and other remedies**
- * Includes new chapters on Negligence, Discrimination Claims and Human Rights Act Claims**

Contents

Introduction: Policing and the Citizen. The Legal Status and Organisation of the Police. The Legal

Status and Organisation of the Police. Complaints Against the Police. Practice and Procedure. Traditional Tort Actions . International Torts to the Person. Police Powers over the Person: Arrest, Detention and Other Miscellaneous Powers. Interfering with Land and Goods. Lawful Justifications for Entry, Search and Seizure. Malicious Prosecution and Related Actions. Other Actions and Remedies. Police Surveillance and Information GatheringIntroduction. Negligence. Misfeasance and other Civil Actions. Discrimination Claims. Judicial Review of Police Decisions. Damages. Other Remedies. The Human Rights Act.

Previous Reviews

As well as being lucid and well-organised, the legal analysis which the authors bring to their work is of a consistently high quality.

Civil Justice Quarterly

For all lawyers involved in such cases, access to this book is a must.

Legal Action

"It has been most impressively researched. Like its predecessors, it will surely prove indispensable to academics and practitioners alike."

The Police Journal

"...a must for anyone interested in this area."

Student Law Journal

"...a definitive source of reference."

The Barrister

"...the third edition has built upon the respected reputation of its predecessors and is fully-up-to-date with the latest Acts of Parliament and leading authorities."

The Barrister

"...those familiar with earlier editions of the work will not be disappointed."

New Law Journal

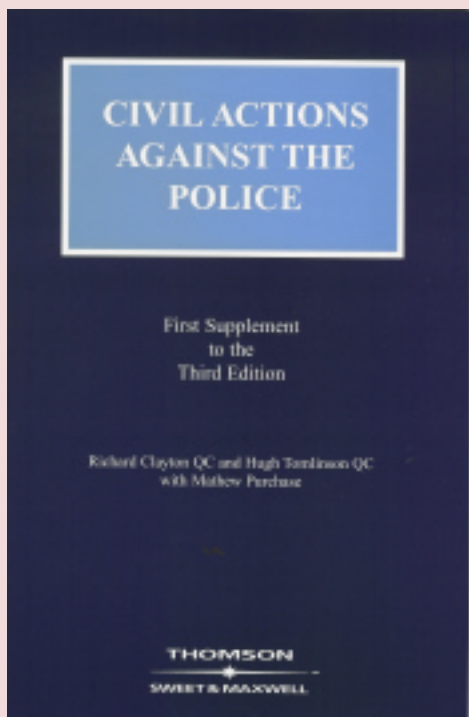
"The book is beautifully presented in quality binding and though expensive, as ever you get what you pay for."

New Law Journal

"a great addition to a chambers' library"

The Barrister

Civil Actions Against the Police First Supplement to the Third Edition



The First Supplement to Civil Actions Against the Police deals with the extensive developments in statute law, regulations and case law since the publication of the Third Edition. The areas covered include:

The far-reaching and controversial changes to police powers brought about by Part 3 of the Serious Organised Crime and Police Act 2005, with numerous amendments to both the Police and Criminal Evidence Act 1984 and the Police Reform Act 2002 and including fundamental re-casting of powers of arrest without warrant

The new complaints system including the Police (Conduct) Regulations 2004 and Police (Complaints and Misconduct) Regulations 2004 and the new Draft Statutory Guidance, Making the New Police Complaints System Work Better

The House of Lords decision in *O'Brien v Chief Constable of South Wales*, on the admissibility of similar fact evidence in police cases

The detailed analysis of the relationship between the tort of false imprisonment and the right to liberty under Article 5 of the ECHR and of police powers in relation to breach of the peace in *Austin v Commissioner of Police for the Metropolis*

The important police negligence decisions by the Privy Council and the House of Lords in *Attorney-General v Hartwell* and *Brooks v Commissioner of Police for the Metropolis*

A series of Court of Appeal decisions relating to police powers of arrest and detention including *R (Laporte) v Chief Constable of Gloucestershire Constabulary*, *Taylor v Chief Constable of Thames Valley Police*, *Cumming v Chief Constable of Northumbria Police* and *Al-Fayed v Commissioner of Police for the Metropolis*

The decision of the Court of Appeal in *Wood v Chief Constable of the West Midlands Police* dealing

with the availability of the defence of qualified privilege in libel cases against the police

The Supplement also contains an Appendix setting out the wide-ranging amend-ments to the Police and Criminal Evidence Act 1984 since the publication of the Third Edition.

REVIEW

Introduction

This book is the first choice book for criminal law barristers and solicitors; police training establishments; lawyers employed by local authorities; regulators; civil rights non-governmental organisations; students; law lecturers and university reference libraries. It is compulsory reference material in any civil action against the police and it focuses on the interplay between civil and criminal law. There is detailed guidance on the most common torts - false imprisonment, malicious prosecution and misfeasance - and clear analysis of developing causes of actions against the police such as negligence, privacy, discrimination and claims under the Human Rights Act.

Why a book about civil actions against the police?

Because there are a range of police problems that need addressing, such as excessive use of physical force; discriminatory patterns of arrest; patterns of harassment of the homeless, youth, racial minorities and gays, including aggressive and discriminatory use of the "stop-and-search" and overly harsh enforcement of petty offences; sometimes verbal abuse of citizens, including racist, sexist and homophobic slurs; discriminatory non-enforcement of the law, such as the failure to respond quickly to calls in low-income areas and half-hearted investigations of domestic violence, rape or hate crimes; illegal spying on political activists; employment discrimination in appointment of police officers, promotion and assignments, and internal harassment of minority, women and gay or lesbian police personnel; use of a "code of silence" or "sending to Coventry" and retaliation against officers who report abuse and/or support reforms; overreaction to gang problems, which is driven by the assumption that those who associate with known gang members must be involved in criminal activity including illegal mass stops and arrests, and demanding IDs from young men based on their race and dress instead of on their criminal conduct; lack of accountability, such as the failure to discipline or prosecute abusive officers, and the failure to deter abuse by denying promotions and/or particular assignments because of prior abusive behaviour; and crowd control tactics that infringe on free expression rights and lead to unnecessary use of physical force. Police have liability under the Animals Act 1971 section 2 (2) (b) if a claimant is bitten by a police dog.

The book includes these important cases-

Keegan v United Kingdom (App 28867/03) and Keegan v Chief Constable of Merseyside [2003] EWCA Civ 936

Obtaining compensation in the European Court of Human Rights for breach of Article 8 and Article 13 following a police search. The court stated, " If the police actions which are the subject of civil proceedings were purportedly done under the authority of a search or arrest warrant, then

procedural difficulties may arise".

Reeves v Commissioner of Police of the Metropolis [2000] 1 A.C.360

The House of Lords considered whether intentional conduct could be within the scope of 'fault' in the Law Reform (Contributory Negligence) Act 1945. The deceased deliberate act of suicide gave rise to a defence of contributory negligence at common law within section 4 of the Act. This appeal concerned a claim for damages against the Commissioner following L's death whilst in custody. It was held that due to the complete control exercised over prisoners in custody by the police, there existed an exceptional duty to prevent self-harm.

Desai v Chief Constable of West Midlands, The Times, May 9, 2000.

The Court of Appeal accepted that a suspect who ignores clear warnings to come out or a dog will be sent to find him, only has himself to blame if he suffers injury as a result. More difficult questions arise when the dog is a police dog trained to act in an unusually fierce way, as in *Gloster v Chief Constable of Greater Manchester Police* [2000] P.I.Q.R, P11.

Osman v UK [1999] 1 F.L.R.193

A leading case in human rights law. This case involved a tragic set of circumstances in which the obsessive former teacher of a 15 year old boy, ultimately wounded his pupil and killed the boy's father. The European Court of Human Rights stated that Article 2 places a positive obligation on the State "to take operational measures to protect an individual whose life is at risk from the criminal acts of another individual".

Goswell v The Commissioner of Police, unreported, April 7, 1998, CA. This case is an important authority on damages.

Legislation affecting civil action against the police.

The Serious Organised Crime and Police Act 2005 brought about a radical shake-up of the organisations and powers to fight major crime - most notably by creating the Serious Organised Crime Agency (SOCA). SOCA brought together the National Crime Squad, the National Criminal Intelligence Service, and parts of the customs and immigration authorities; it will have approximately 5,000 civilian staff with powers to arrest and carry out their own investigations. The Act overhauls the powers of the police officers contained in the Police and Criminal Evidence Act 1984 - in particular by introducing new 'supergrass' provisions dealing with the use of informant evidence. The Act introduces new public order offences in relation to harassment and protest. The Protection from Harassment Act 1997 is designed to tackle a wide variety of forms of harassment. In particular: Section 4 relates to putting people in fear of violence which applies if a person pursues a course of conduct which they know or ought to have known causes another to fear that violence will be used against them. Section 2 is a lower level offence where a person pursues a course of conduct which they know or ought to have known causes harassment. Section 5 relates to restraining Orders available from the criminal courts which prohibit further harassment or conduct which causes fear of violence. A breach of this order is a criminal offence. The Protection from Harassment Act 1997 had been used to protect employees and persons from harassment, notably in connection with work

that has involved the use, or treatment, of animals. The Act was primarily intended to be used to combat “stalking” but the provisions are not limited to that conduct. The amendments introduced by section 115 of the Serious Organised Crime and Police Act 2005 aim to make the legal position clearer. Section 125 of SOCPA amends the 1997 Act by inserting a new subsection 1 of the 1997 Act and it also inserts a new subsection 3A.

Section 113 of the Serious Organised Crime and Police Act 2005 states that PACE is amended as follows:-

Section 8 {power to authorise entry and search of premises) is amended as provided in subsections (3) and (4); in subsection (1), subsection (15);subsection (6)...and SOCPA section 132, on demonstrating without authorization in a designated area also makes for more cases of civil action against the police.

New Police Complaint System

The police operate on the principle that they can only carry out their duties if they have the agreement and support of the community. To ensure a good relationship between the police and the public, it is important that there is a fair and thorough system for complaining.

Since 1 April 2004 a new independent police complaints organisation has been in place, the Independent Police Complaints Commission. For the first time, police complaints can be conducted by independent investigation teams, people complaining have more rights and the whole complaints process now has stricter standards. Complaints can be made about police officers who neglect their duty; drink on duty; use racist behaviour or language; are involved in corrupt practices; use excessive force.

All these are essential reasons for this comprehensive volume, "Civil Actions against the Police".

Sally Ramage

"CIVIL ACTIONS AGAINST THE POLICE", by R.Clayton & H.Tomlinson, Sweet & Maxwell, London, 2006.

An Extended Review by Sally Ramage

What Does it Provide?

"Civil Actions against the Police" provides comprehensive analysis of the civil rights and remedies for police misconduct. It covers complaints against the police as well as the practice and procedure of bringing a claim. It provides detailed explanation on the traditional tort actions that may be brought against the police as well as the developing tort of misfeasance in public office and claims in breach of confidence and data protection. Covering all possible actions against the police in one place, it provides detailed procedural guidance - ensuring practitioners have all the information they need when preparing a civil action. It includes all the relevant documents - including PACE Codes and JSB Specimen Directions, covers damages and other remedies, and includes new chapters on Negligence, Discrimination Claims and Human Rights Act Claims. It provides clear

and practical guidance in those areas where negligence liability has been decided, and academic analysis where those aspects of the law are unclear or developing.

Why a Book about Civil Actions Against the Police?

Because there are a range of police problems that need addressing, such as excessive use of physical force; discriminatory patterns of arrest; patterns of harassment of the homeless, youth, racial minorities and gays, including aggressive and discriminatory use of the "stop-and-search" and overly harsh enforcement of petty offences; sometimes verbal abuse of citizens, including racist, sexist and homophobic slurs; discriminatory non-enforcement of the law, such as the failure to respond quickly to calls in low-income areas and half-hearted investigations of domestic violence, rape or hate crimes; illegal spying on political activists; employment discrimination in appointment of police officers, promotion and assignments, and internal harassment of minority, women and gay or lesbian police personnel; use of a "code of silence" or "sending to Coventry" and retaliation against officers who report abuse and/or support reforms; overreaction to gang problems, which is driven by the assumption that those who associate with known gang members must be involved in criminal activity including illegal mass stops and arrests, and demanding photo IDs from young men based on their race and dress instead of on their criminal conduct; lack of accountability, such as the failure to discipline or prosecute abusive officers, and the failure to deter abuse by denying promotions and/or particular assignments because of prior abusive behaviour; and crowd control tactics that infringe on free expression rights and lead to unnecessary use of physical force.

Specific civil action cases against the police.

The most usual claims brought are claims for assault, false imprisonment, malicious prosecution, and claims damages.

In a claim for assault it will be necessary to prove that the police used an unreasonable level of force. The police are entitled by law to use a reasonable degree of force appropriate to the circumstances they are in, but they are not entitled to use excessive force and if they do so they are open to be criticised that they have committed an assault. An Assault can also include being bitten by police dog.

In a false imprisonment claim, it will be necessary to prove that the police had no reasonable information to suspect the claimant of having committed an offence and to detain him in relation to that offence. It is not for the police to decide whether he is guilty or not. It is for them to decide whether there is a criminal case that should be put before the court to decide whether he is guilty or not. If there was no reasonable information then the arrest can be challenged as unlawful and if successfully challenged damages may be awarded based on the time spent in custody.

In a claim for malicious prosecution it will be necessary to establish that the primary motive in pursuing the prosecution was something other than the interests of justice. It must be proved that the police had a wrongful motive in prosecuting you. Such a civil claim for damages against a police force will be brought in either the High Court or the County Court.

In arresting a person, the arresting officer must indicate that the arrest is taking place and give a

reason for it. This was made clear in *Christie v Leachinsky* (1947) and confirmed by article 30 of the PACE Order. If it later turns out that the reason for the arrest was not a good one, the person arrested can claim compensation for "false imprisonment" and "malicious prosecution".

Funding Civil Actions Against the Police.

Legal Aid is available to pursue complaints and claims against the police and other public authorities for assault, false imprisonment and malicious prosecution. To obtain a funding certificate for court proceedings there is a two fold test. The first part is an income based test to see whether the applicant's income qualifies him for funding. The second part of the test is a merit test to assess whether the claim is strong enough to warrant use of the public fund. The prospective plaintiff's solicitor advises the Legal Services Commission on this element.

Some Relevant Cases.

Keegan v United Kingdom (App 28867/03):- Obtaining compensation in the European Court of Human Rights for breach of Article 8 and Article 13 following a police search.

Goswell v The Commissioner of Police, unreported, April 7, 1998:- appeal against record award of damages against the Police.

Sinclair v The Metropolitan Police, unreported, June 2000:- sex discrimination.

Keegan v Chief Constable of Merseyside Police [2003] 1 WLR 2187:- Appeal raising ambit of tort of malicious procurement of search warrant in circumstances where no human rights claim could be brought.

Wilson v. Commissioner of Police for the Metropolis, unreported, 2002:- This is the highest award of damages for a claim of this type. The Claimant was a 16 year old boy who was struck on the head by an unidentified riot police officer. The claimant suffered a fractured skull causing disrupted education and career prospects. The case was dropped by the previous legal team who described it as "a hopeless case". Legal aid funding was then discharged. In June 2000 James successfully reapplied for legal aid and re-interviewed witnesses. The Defendant made several applications to have the case struck out on technical grounds but the case finally got to trial in July 2001. The claimant won the trial Judge Mr Justice Morland declaring that the incident was "a deliberate unlawful assault." The Metropolitan Police took the case to the Court of Appeal but their appeal was dismissed. Following this a further series of interim applications were the issued by both sides dealing with issues of medical evidence and the costs of future care. The claim was settled by negotiation for the sum of £500,000 2 weeks before the assessment of damages hearing in July 2002. The Claimant had been unable to identify the officer who attacked him and was unable to formally complain as it was not possible under the Police Act 1996 to complain about an unidentified officer. The Police Reform Act 2002 now allows such a complaint to be investigated.

Douglas v. Commissioner of Police for the Metropolis, unreported, 2004:- Claim settled for damages brought by Mr Douglas in the High Court for Assault, False Imprisonment and Malicious prosecution. On 6 January 1998 having left a garage where work was being undertaken on his

motor vehicle, he agreed to share a minicab with a stranger. A short distance down the road Mr Douglas left the minicab to buy some cigarettes and upon his return to the minicab found the occupants being searched by plain clothes police officers. It would appear that Crack Cocaine was found in the possession of the other man. Mr Douglas alleges that he was sworn at, pushed and told to go away and when he did not, uniformed officers were summoned to the scene and conveyed Mr Douglas to the Brixton Police Station, the arresting officers arriving some 8 minutes later. At the Police Station it was claimed that Mr Douglas had walked up to them and simply dropped 20 rocks of Crack Cocaine in front of them, at which point the arresting officer handcuffed him. Mr. Douglas immediately protested that he was being "set up" by the officers, but his complaints were ignored. His detention was authorised and he was manhandled to a detention room where he alleges he was further assaulted. During the course of a further purported search in the detention room, the officers concerned claimed to recover one further rock of Crack Cocaine from Mr Douglas. Mr Douglas denied this. Mr Douglas remained in detention for 44 hours, throughout which he maintained his innocence and repeated his allegations that he was being "set up". Mr Douglas was charged with conspiracy to supply Crack Cocaine, possession with intent to supply Crack Cocaine and possession of Crack Cocaine. He was remanded into custody pending trial. At the Inner London Crown Court in May 1998 Mr Douglas was acquitted of all offences. Mr Douglas then commenced a civil claim for damages against the MPS before transferring his case to Christian Khan in 2002. Despite difficulties in securing CCTV evidence of events at the Police Station, proceedings were issued and the matter vigorously defended. The CCTV was eventually obtained under Court Order and raised issues as to whether more officers were involved in the alleged corruption than had originally been believed to be the case, and whether more drugs had been recovered from the scene by the officers than were later handed in at the Police Station. The CCTV also appeared to show evidence of a conspiracy by a number of officers, including three sets of handcuffs having been on Mr Douglas, none of which appeared to belong to the arresting officer. The trial was listed for 1 November 2004, however, 10 days before, the Metropolitan Police Service settled Mr Douglas' claim for £40,000.00.

Osman v UK [1998]29 E.H.R.R.212: - A leading case in human rights law. This case involved a tragic set of circumstances in which the obsessive former teacher of a 15 year old boy, ultimately wounded his pupil and killed the boy's father. The applicants had demonstrated that in the months before the fatal attack the police had been given information that should have made clear the extent of the danger of assault. Despite such information being made available to the police the suspect's home had not been searched, nor had any special measures been put in place to protect the Osman family. The High court, Court of Appeal and the House of Lords agreed that Metropolitan Police owed no duty of care to the Osman family. They confirmed the decision given in *Hill v Chief Constable of West Yorkshire Police (1989)*. In this case the father of a woman murdered by Peter Sutcliffe attempted to sue Yorkshire police. The family claimed the police missed numerous opportunities to catch the perpetrator of these crimes. The UK courts decided that the police did not owe a duty of care to any individual member of the public. The case was decided on so called public policy grounds meaning that even if the police were at any point negligent in the way in which investigations or protection was provided, public policy would prevent any such case coming to court. The European court found that that Article 6 of the European convention on Human rights (the family's Right to a Fair Trial) had been breached. They effectively ordered that this blanket

ban should be overturned.

Earl Hill v Commissioner of Police, Goswell v Commissioner of Police (4/11/98, CCRTF97/1558/2):- This case is an important authority on damages.

R v Governor of Brockhill Prison ex parte Evans (no. 2) [2001] 2 AC 19:- Establishes that any unlawful detention gives rise to a damages claim.

Reeves v Commissioner of Police for the Metropolis[2000] 1 A.C.360:- This appeal concerned a claim for damages against the Commissioner following L's death whilst in custody. It was held that due to the complete control exercised over prisoners in custody by the police, there existed an exceptional duty to prevent self harm.

Slater-v-Commissioner of the Metropolitan Police [1996] Times Law Reports 23.1.1996:- A claim involving title to monies found in a drug factory and the application of "ex turpi causa" maxim.

Orange v Chief Constable of West Yorkshire (2001:- This appeal concerned Orange's claim in negligence for damages following the suicide of her husband, the deceased having hanged himself whilst in police custody.

R (Ellis) v Chief Constable of Essex, unreported,(2003:- The case concerned the lawfulness of a police scheme whereby poster's showing the names and photos of offenders would be displayed in public. The court held that the lawfulness was dependent upon individual circumstances as well as upon how the scheme would operate in practice.

R (on the application of Gillan) v Commissioner of Police for the Metropolis, unreported, 2004:- The case concerned the lawfulness of stop and search decisions pursuant to the Terrorism Act 2000 where the Appellants had been stopped on their way to a demonstration.

McGrogan v Chief Constable of Cleveland [2002] EWCA Civ 86:- police power to detain for the purpose of preventing further breach of peace.

O'Brien v Chief Constable of South Wales [2003] EWCA Civ 1085:- The case concerned the admission of evidence in a claim for malicious prosecution and misfeasance in public office, where the Claimant had served 11 years of a life sentence for murder before his conviction was quashed on appeal.

R (application Clare) v Independent Police Complaints Commission [2005] 1 Pol LR 185 establishes that IPCC is permitted to withdraw a dispensation from a requirement to investigate a complaint.

Paul v Chief Constable of Humberside Police [2006] EWCA Civ 1433:- Out of time appeal by CC Humberside Police not allowed.

Jason Paul v Chief Constable of Humberside Police, unreported, January 27,2006:- Civil claim against the police. Establishes that claims for damages against the police will often involve drawing inferences against the police evidence. Jason Paul, wrongly accused by the police of assaulting Christopher Alder before Mr Alder was unlawfully killed in police custody, has today won his civil

claim against the police at the second attempt. Mr Paul brought a claim for false imprisonment and malicious prosecution after he was arrested for murder and detained on 1st April 1998. He was awarded damages plus legal costs. The two week trial in front of a jury in Sheffield followed a ruling in March 2004 by the Court of Appeal that the judge at the first trial was wrong to withdraw the case from the jury and throw out the claim - see 'Court of Appeal Orders Re-trial of Jason Paul's civil action against the Police'

Ongoing Civil Action against South Wales Police by mother of child abducted and raped by Craig Sweeney in 2006:- A senior inspector and a superintendent from South Wales Police now face a misconduct panel for failing in their duties. A third officer involved in the case has since retired and will face no further action. The family said later that they were launching a civil action against the police for their "failure to protect our child from a known and dangerous child molester". In spite of the mother's phone call to police, Sweeney, 24, drove his victim back to his flat on Caerleon Road, Newport, and repeatedly sexually assaulted her. He was caught by chance only after a high-speed chase in Wiltshire after local police saw him ignoring a red traffic light with his car headlights switched off.

Legislation Affecting Civil Action Against the Police.

The Serious Organised Crime and Police Act 2005 brought about a radical shake-up of the organisations and powers to fight major crime - most notably by creating the Serious Organised Crime Agency (SOCA). SOCA brought together the National Crime Squad, the National Criminal Intelligence Service, and parts of the customs and immigration authorities; it will have approximately 5,000 civilian staff with powers to arrest and carry out their own investigations. The Act overhauls the powers of the police officers contained in the Police and Criminal Evidence Act 1984 - in particular by introducing new 'supergrass' provisions dealing with the use of informant evidence. The Act introduces new public order offences in relation to harassment and protest. The Protection from Harassment Act 1997 is designed to tackle a wide variety of forms of harassment. In particular: Section 4 relates to putting people in fear of violence which applies if a person pursues a course of conduct which they know or ought to have known causes another to fear that violence will be used against them. Section 2 is a lower level offence where a person pursues a course of conduct which they know or ought to have known causes harassment. Section 5 relates to restraining Orders available from the criminal courts which prohibit further harassment or conduct which causes fear of violence. A breach of this order is a criminal offence. The Protection from Harassment Act 1997 had been used to protect employees and persons from harassment, notably in connection with work that has involved the use, or treatment, of animals. The Act was primarily intended to be used to combat "stalking" but the provisions are not limited to that conduct. The amendments introduced by section 115 of the Serious Organised Crime and Police Act 2005 aim to make the legal position clearer. Section 125 of SOCPA amends the 1997 Act by inserting a new subsection 1 of the 1997 Act and it also inserts a new subsection 3A.

Section 113 of the Serious Organised Crime and Police Act 2005 states that PACE is amended as follows:-

"Section 8 {power to authorise entry and search of premises) is amended as provided in subsections

(3) and (4); in subsection (1), subsection (15);subsection (...".

SOCPA section 132 on demonstrating without authorization in a designated area also makes for more cases of civil action against the police.

New Police Complaint System.

The police operate on the principle that they can only carry out their duties if they have the agreement and support of the community. To ensure a good relationship between the police and the public, it is important that there is a fair and thorough system for complaining.

Since 1 April 2004 a new independent police complaints organisation has been in place, the Independent Police Complaints Commission. For the first time, police complaints can be conducted by independent investigation teams, people complaining have more rights and the whole complaints process now has stricter standards. Complaints can be made about police officers who neglect their duty; drink on duty; use racist behaviour or language; are involved in corrupt practices; use excessive force.

You can complain about any police officer or any other member of police staff, such as a special constable, community support officer. It is to be noted that if you make a false complaint you may risk being prosecuted for defamation, libel, or for wasting police time.

A complaint can be made orally at the police station. In a or written account to the Chief Constable of that police Headquarters or by writing directly to the Police Complaints Authority, 10 Great George Street, London, SW1P 3AE, who will forward your complaint to the correct police force. The letter must include details of what happened, when it happened, who was involved, what was said or done, the names of any witnesses, other than yourself and the officer, where the witnesses can be contacted, what proof, if any, exists of any damage or injury.

The police force whose officers have been complained about must decide whether to record a complaint. If an informal approach is not acceptable, or if the complaint raises certain more serious allegations, it must be fully investigated by a senior police officer. Police forces must notify the most serious complaints to the Police Complaints Authority as soon as they are recorded. The Authority must, by law, supervise certain investigations and in others they may choose to do so. The Authority approves the appointment of the Investigating Officer, decides how the inquiry should be carried out, reads all the statements and sees all the evidence. The final report goes to the Authority which states whether it was satisfied or not with the way the investigation was carried out. After the investigation, the Crown Prosecution Service will decide whether any criminal charges will be brought against police officers. The Police Complaints Authority then decides whether or not any police officers should face misconduct proceedings. Action can only be taken if it can be proved that an officer has breached the Police Codes of Conduct. If there is a misconduct hearing, the police will inform the complainant who may be asked to attend. Making a complaint does not affect the right to take the police to court and sue for damages.

General Comment on Actions Against the Police.

Police abuse is a serious problem. It has a long history, and it seems to defy all attempts at eradication. The problem is national in that no police department in the country is known to be completely free of misconduct. However, policing has seen much progress.

Human Rights.

It is all very well to have laws on human rights, but if those laws are imperfectly enforced they may as well not exist. The European Convention on Human Rights can be enforced by individuals in the European Commission of Human Rights and then, provided the application is referred to it, in the European Court of Human Rights

REFERENCES.

A.C.P.O. (1998) 'Sexual Orientation: A Reference Document for the Police Service', London, HMSO.

R.Clayton and H.Tomlinson, Civil Action against the Police, Sweet & Maxwell, (London 2005)

Douglas, Nicola et al., 'Playing it Safe: Responses of Secondary School Teachers to Lesbian, Gay and Bisexual Pupils, HIV and AIDS Education and Section 28', University of London Institute of Education, (London 1997)

Greater Manchester Lesbian and Gay Policing Initiative, 'Lesbians Experiences of Violence and Harassment', (Manchester 1999)

Health Education Authority, 'Health update: Sexual Health', HEA, (London 1996)

I. Rivers, "Researching Bullying and Education Systems: It's Not Just About Bullying, It's About Survival", paper presented at 42nd Street Conference, 'Inside Out' Manchester, 27th March 1998.

The National Advisory Group, "Breaking the Chain of Hate: A National Survey Examining Levels of Homophobic Crime and Community Confidence towards the Police Service", (Manchester 1999)

L.Trenchard, and H.Warren, "Something To Tell You: The Experiences and Needs of Young Lesbians and Young Gay Men in London", London Gay Teenage Group, 1999.

K. B. Mamula, "City files civil action over police records system dispute," Tribune Review, Greensburg, PA, February 20, 1998.

B. Harden, "Civil rights investigation targets N.Y. Police," Washington Post, August 19, 1997.

J. Percival, "Family sue police over Sweeney sex attack failures", Times Newspaper, July 26, 2006

"Revisiting the caselaw R v KHAN [\[1\]\[1\]](#) (1996) The Times, July 5 House of Lords"

By Sally Ramage

February 2007

In light of the Interception of Communications (Admissibility of Evidence) Bill 2007, it is a good idea to revisit R v Khan and examine the issue of interception of communications as a privacy issue.

To refresh on the facts of R v Khan, Khan had arrived from Pakistan at Manchester airport on the same flight as his cousin Nawab. When stopped and searched, Nawab was found to be in possession of heroin with a very high street value. He was interviewed, arrested and charged. No drugs were found on Khan who made no admissions on interview and was released without charge.

Later Khan was in Sheffield, at the home of a man named Bashforth. Police installed a listening device outside. Neither Khan nor Bashforth was aware of its presence. The police obtained a tape recording of a conversation. In the course of the conversation, Khan made statements which amounted to an admission that he was a party to the importation of drugs by Nawab.

He was arrested and jointly charged with Nawab. The judge admitted the intercept evidence and Khan was re-arrested and pleaded guilty to being knowingly concerned in the fraudulent evasion of the prohibition on the importation of heroin.

The Court of Appeal dismissed his appeal.

This case raised issues of whether the evidence was admissible and if admissible, whether it should have been excluded by the judge in the exercise of his discretion under common law or S.78 PACE 1984.

There was no legal framework regulating the installation and use by the police of covert listening devices. In the light of R v Sang [1980] AC 402, the argument that the evidence of the taped conversation was inadmissible could only be sustained if two wholly new principles were formulated: The first would be that Khan enjoyed a right of privacy in respect of the taped conversation. The second that evidence of the conversation obtained in breach of that right was inadmissible.

There was no such right of privacy in English law, and even if there were, evidence obtained improperly or even unlawfully remained admissible, subject to the judge's power to exclude it at his discretion.

If the circumstances in which the evidence was obtained amounted to an apparent invasion of Khan's rights of privacy under article 8, that was accordingly something to which the court must have regard.

The sole cause of the case coming to the House of Lords was the lack of a statutory system regulating the use of surveillance devices by the police.

The Privacy Issue

Currently, privacy is a sweeping concept, encompassing freedom of thought, control over one's

body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. What must be borne in mind when thinking about the meaning of privacy is that when we protect privacy, we protect against disruptions to certain practices. A privacy invasion interferes with the integrity of certain practices and even destroys or inhibits such practices. "Privacy" is a general term that refers to the practices we want to protect and to the protections against disruptions to these practices. Privacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the practice of which it is a part.

What does it mean when we say that these aspects of life are "private"? This question is very important for making legal and policy decisions. Many recognize the importance of privacy for freedom, democracy, social welfare, individual well-being, and other ends. Many also assert it is worth protecting at significant cost. Society's commitment to privacy often entails restraining or even sacrificing interests of substantial importance, such as freedom of speech and press, efficient law enforcement and access to information. . The use of the word "privacy" constitutes the ways in which we employ the word in everyday life and the things we are referring to when we speak of "privacy." The word "privacy"[2] is currently used to describe a myriad of different things:- freedom of thought, control over personal information, freedom from surveillance, protection of one's reputation, protection from invasions into one's home, the ability to prevent disclosure of facts about oneself, and an almost endless series of other things.

However, most people fail to understand how privacy should be valued vis-à-vis other interests, such as free speech, effective law enforcement, and other important values.

As the UK has no privacy law, let us look to the US to see how their law treats privacy. In *Olmstead v. United States*, the Court held that wiretapping was not a violation under the Fourth Amendment because it was not a physical trespass into the home. But, in 1967, the Court swept away this view in *Katz v. United States*, holding that the Fourth Amendment did apply to wiretapping. In *California v. Greenwood*, the Court held there is no reasonable expectation of privacy in garbage because it is knowingly exposed to the public.

In *Florida v. Riley*, the Court held that the Fourth Amendment did not apply to surveillance of a person's property from an aircraft flying in navigable airspace because the surveillance was conducted from a public vantage point.¹

The fact that the tape recording in *R v Khan* was between two persons can illustrate that privacy cannot be pleaded since a person other than Khan had rights to the conversation, as illustrated by the US case, *Haynes v. Alfred A. Knopf, Inc.*

This case involved Nicholas Lemann's book about the social and political history of African Americans who migrated from the South to northern cities. The book chronicled the life of Ruby Lee Daniels, who suffered greatly from her former husband Luther Haynes's alcoholism, selfishness, and irresponsible conduct. Haynes sued the author and the publisher under the public disclosure of private facts tort, claiming that he had long since turned his life around and that the

disclosure of his past destroyed the new life he had worked so hard to construct. Judge Posner, writing for the panel, concluded that there could be no liability for invasion of privacy because a person does not have a legally protected right to a reputation based on the concealment of the truth and because the book narrated a story not only of legitimate but of transcendent public interest. Although it did not hinge on the shared nature of the information, this case illustrates that personal information rarely belongs to just one individual; it is often formed in relationships with others. Ruby Daniels's story was deeply interwoven with Haynes's story. Daniels had a right to speak about her own past, to have her story told. This was her life story, not just Luther Haynes's.

As early as 1891, the US Court articulated this conception in *Union Pacific Railway Co. v. Botsford*. In holding that a court could not compel a plaintiff in a civil action to submit to a surgical examination, the Court declared the sanctity of the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.

As to interception of communication with regard to the home, the US courts have always treated this as a breach of privacy. As early as 1886, in *Boyd v. United States*, the US Court strictly protected the sanctity of a man's home. The maxim that the home is one's castle appeared as early as 1499. The first recorded case in which this notion was mentioned was *Semayne's Case*^{[2][2]}. In the eighteenth century, William Blackstone declared that the law has "so particular and tender a regard to the immunity of a man's house that it styles it his castle, and will never suffer it to be violated with impunity." ^{[3][3]}

However, today's Information Age often involves exchanging information with third parties, such as phone companies, internet service providers, cable companies, retailers, and so on. And so, clinging to the ancient notion of privacy as related in the previous paragraph, would mean the practical extinction of privacy in today's world. In contrast to the notion of privacy as secrecy, privacy can be understood as an expectation in a certain degree of accessibility of information.

Biometric technologies are changing society and the European Commission's Report of February 2007 into the impact of such technologies, concluded that the burgeoning information society brings with it the need for us to be able to securely identify ourselves quickly and remotely and therefore we need the inevitable implementation of biometric technologies to increase national security, and as a tool to help prevent fraud^{[4][4]}. We read half-baked alarmist articles about interception of communications and breach of privacy yet we in the UK are behind other countries where "intercepting communications" are concerned. It is to be noted that in the US, more than three million customers regularly pay for goods and services just by scanning their fingers and punching in a personal identification number (PIN) instead of using a credit or debit card. In Japan, more than two million people now use contact-less palm-scanners to withdraw cash from a bank cash-point. Many laptop computers now have built-in finger scanners. There are now biometric front door locks, garage doors and safes, proving that this is not a 'big brother' technology but that we are in the information age. And there are fingerprint scanners that detect fake fingers.

In *U.S. West, Inc. v. Federal Communications Commission*, a telecommunications carrier challenged the privacy regulations of the Federal Communications Commission ("FCC"), which

restricted the use and disclosure of customers' personal information unless the customers gave their consent. The court stated that a "general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest, for it is not based on an identified harm. Our names, addresses, types of cars we own, and so on are not intimate facts about our existence, certainly not equivalent to our deeply held secrets or carefully guarded diary entries. In cyberspace, most of our relationships are more like business transactions than intimate interpersonal relationships."

In the UK today, if recordings are secret, they are still inadmissible in civil cases, as per *Chairman and Governors of Amwell School v Dogherty*, Employment Appeal Tribunal, 5th October 2006. It was decided that unauthorised recordings made by a claimant, of the private deliberations of her employer's disciplinary hearing panel, should not be admitted as evidence in support of her unfair dismissal claim at an employment tribunal on the grounds of public policy. Mr Recorder Luba, QC, said that there was an important public interest, in parties before disciplinary proceedings complying with the ground rules on which the proceedings were based and that no ground rule could be more essential to ensuring a full and frank exchange of views than the understanding that their deliberations would be conducted in private.

This case is a far cry from *R v Khan*, a serious criminal case of drug trafficking. Possession with intent to supply is determined in the Misuse of Drugs Act 1971, section 5(3) and carries life imprisonment and/or fine in relation to class A drugs. The two situations are incomparable.

Besides, the UK Regulation of Investigatory Powers Act 2005 contains far-reaching powers on telecommunications interception and a decryption order relationship between less privacy and more security.

The UK Terrorism Act enables the police to carry out surveillance to prevent terrorism. But surveillance under the UK Terrorism Act is a minor thing compared to the US's Patriot Act 2001. These are some of the surveillance that the Patriot Act allows:-

A nationwide search warrant.

For electronic evidence (ie wire, oral or electronic communications or stored in a remote computer service as described by the Federal wiretap law), nationwide authorizations are obtainable.

Delayed notice of a search warrant is allowed.

Government agencies share information.

The Patriot Act provides for immunity defences for Internet Service Providers when ISPs comply with surveillance and disclosure orders, enabling the government to intercept communications of "computer trespassers".

Voicemails may be seized via search warrants.

There can be sharing of intercepted information between agencies, voluntary emergency disclosure

of the contents of subscriber communications and records by an ISP and mandatory disclosure pursuant to a court order or warrant.

Also, under the US Foreign Intelligence Surveillance Act, there can be multi-point wiretaps.

My conclusion on the alleged dichotomy between privacy and interception of communications as criminal evidence, is that, if the 2007 Bill Interception of Communications is passed, it will put these intercepts on a statutory footing and save much time and money when cases such as R v Khan are no longer feasible.

Sally Ramage

Trafficking Update 2007

Sally Ramage

In 2003 UK police were saying that trafficked women who were in the prostitution industry were there because they wanted to be there.

Things have moved a long way forward since that time. The Vice Squad now have statistics and much more evidence about the organised crime of trafficking. In the UK, there are 86,000 prostitutes and of these, an estimated 4,000 are trafficked women. It can be said that 82,000 of these women are internally trafficked and 4,000 women are externally trafficked.

(Historically, women have always been in subjugation, as evidenced by writings such as these: Thomas Clarkson (1760-1846) wrote "Is it lawful to make slaves of others against their will?" Josephine Butler (1828-1906) wrote, "We need to resist the tacit agreement which leaves men free to purchase and procure whilst women themselves are in chains".)

The UK police now know the answers to these questions, though they may not have adequate budgets to fully tackle these issues:-

- 1. Where is the power located in the sex industry?**
- 2. What are the gender, age, ethnicity and distribution of this power?**
- 3. What hidden violence is submerged in the various businesses of selling 'flesh'?**

The global sex industry is worth some 7 to 12 billion US dollars each year and

this money feeds directly into the black economy of illicit drugs, illegal immigration and terrorism. It is highly organised crime. There are 900,000 to 1 million trafficked prostitutes in the world, according to statistics by the US State Department. The minimum worth of the sex industry can be quickly calculated with the knowledge that these 86,000 prostitutes ply their craft in minimum 10 hour days, six days each week, at a minimum of £25 a customer for a maximum of 20 minutes. They

work 6 days a week, and even allowing for overheads, must make their owners about £193 million a year in the UK alone, and tax free.

There has been progress made in the UK in so far as the UK government has signed and ratified the Palermo Protocol.

Research has found that there is no trafficking of males for prostitution and that men

who practice in this area in a similar fashion to prostitutes in brothels, do so from the groups of asylum seekers who fail in their claims, etc. Research in this area shows that such men are well organised themselves and carry out prostitution in houses, with a cleaner and administrative facilities in place- they organise themselves in this crime whilst women are managed by organised criminals.

Today, trafficked women used for prostitution come from 3 main regions of the world. Women who are trafficked from Cameroon, Ghana, Uganda, Nigeria and the Sudan work in secure suburban houses in groups so as not to attract attention. The brothel prostitutes who were trafficked usually come from Lithuania, Ukraine, Romania, and Moldavia. There is another group of women mainly from Vietnam, China, Thailand, India and Pakistan. It has been noted that another group are beginning to be trafficked from South America.

The crux of the crime though, is the demand side. Men want to pay for this type of sex, understanding full well that someone else's body can be owned (temporarily) for money. This occurs all over the world including the United Kingdom. Research has discovered that the sex market is growing in Italy, France, Belgium, Germany, Japan, Canada and the USA.

The UK government really began to take the matter seriously after Operation Pantameter, when 82 prostitutes were arrested in Manchester brothels and taken and debriefed.

What is the main criminal element in all this trafficking? Deception.

One heartening development is that, where there was just the Poppy charitable organisation in 2003 to help such trafficked persons, there are now other organisations offering help- such as the Salvation Army, the Medialle Trust, the Baptist Church and ChasTe.

Be Vigilant Against Identity Theft

By Sally Ramage

The UK's Identity Cards Act 2006 establishes that there must be a register of individuals in the UK and this is to be known as the National Identity Register, to be established and maintained and confined to the statutory purposes. The statutory purposes are stated in section 1(3) of the Act as :-

'(3) The statutory purposes are to facilitate, by the maintenance of a secure and reliable record of registrable facts about individuals in the United Kingdom

the provision of a convenient method for such individuals to prove registrable facts about themselves to others who reasonably require proof; and

the provision of a secure and reliable method for registrable facts about such individuals to be ascertained or verified wherever that is necessary in the public interest.

Section 1 (4) of the Act defines what is necessary in the public interest, the top purpose being ‘in the interests of national security’, second being ‘for the purposes of the prevention or detection of crime’.

It is hoped that this article reveals just how necessary this is and just how vulnerable we are without such legislation, by examining the situation in the United States, a much bigger place than the UK, and ahead of the UK as far as monitoring the significance of the electronic age in relation to national security.

According to cyber-security experts, the terror attacks of 11 September and 7 July could be seen as mere staging posts compared to the havoc and devastation that might be unleashed if terrorists turn their focus from the physical to the digital world. [\[5\]\[1\]](#).

Scott Borg, the director and chief economist of the US Cyber Consequences Unit (CCU), a Department of Homeland Security advisory group, believes that attacks on computer networks are poised to escalate to full-scale disasters that could bring down companies and kill people. He warns that intelligence chatter increasingly points to possible criminal or terrorist plans to destroy physical infrastructure, such as power grids. Al-Qa’ida, he stresses, is becoming capable of carrying out such attacks.

Most companies and organisations seem oblivious to the threat. Usually, they worry about e-mail viruses and low-grade hacker attacks. However, Borg sees these as the least of their worries. Up to now, executives and network professionals have worried about what adolescents and petty criminals have been doing. In most cases, these kinds of cyber attacks are not very destructive. The reason is that businesses generally have enough inventory and extra capacity to make up for any short-term interruptions.

What companies and organisations should worry about is what terrorists or hardcore criminals could do... One key target would probably be the vital Supervisory Control and Data Acquisition (Scada) systems in power plants and similar industries in the USA. ‘Chatter’ on Scada attacks are increasing, evident by patterns of behaviour that suggest that criminal gangs [\[6\]\[2\]](#) and militant groups are now fully capable of unleashing such attacks.

Control systems are a worry because these are the computer systems that manage physical processes. They open and shut the valves, adjust the temperatures, throw the switches, regulate the pressure... The control systems for chemical plants, railway lines, or manufacturing facilities are the systems to worry about, as also are electronic evidence-capturing systems to comply with a country’s evidence rules. Shutting these systems, down is a nuisance. Causing them to do the wrong thing at the wrong time is much worse.

Until now, hackers have usually targeted credit cards or personal information on the web. More

sophisticated hackers, however, are beginning to focus on databases. The type of data most likely to be hit, Borg says, might include a pharmaceutical company's drug development databases, or programs that manipulate data, such as formulas for generating financial statements.

Many attacks of this kind would have two components. One would alter the process control system to produce a defective product. The other would alter the quality control system so that the defect would not easily be detected, say the experts. This would cause sheer panic if, for instance, a life-saving drug were produced but distributed in incorrect dosage, causing deaths and disability. People would become afraid of having to go to hospitals, not to mention large numbers of litigants that would ensue. In this same way, travesties due to incorrect online saboteurs could change key specifications at a car factory, resulting in accidents such as causing a vehicle to burst into flames, say, after it had been driven for a certain time. The VEHICLE MANUFACTURER would PERISH... A few such attacks, run simultaneously, would send economies crashing. Populations would be in turmoil. In addition, at the click of a mouse, the terrorists would have won.

Intelligence reports in the past year are a worrying read... An assessment by the British security service MI5 reported that Britain is not far removed from anarchy... The greatest fears about electronic attacks focus -on the more exposed networks that make up the critical national INFRASTRUCTURE.

A breach of a person's privacy when hackers steal information, The Business intelligence Industry expects to churn out tools that appeal to a broad audience. With steady interest from database vendors and other large companies interested in acquiring specialty business intelligence, hackers are breaching Privacy Laws. Hackers are intercepting networks, but just by 'plugging in a box' [[7][3]] 'plug-and-play' device, can stop total-flow traffic inspection at multi-Gigabit speeds. As the number of business intelligence users swell and as corporate buyers insist that the technology will break free of its limited use among data analysts and specialists, there will be attempts to rope in average corporate knowledge workers, supply chain partners and customers. Similarly, there will be 'plug and play' devices to gain business intelligence, or steal information, even by mainstream users with less-complicated querying techniques and basic and yet creative ways of presenting information gleaned from business intelligence and data warehousing tools. As business intelligence users increase rapidly, so the number of vendors serving up spying systems could diminish due to company mergers. as the huge database suppliers take over small business intelligence vendors

.Business Intelligence equipment is being brought to the mass market and with it, there are concerns are that terrorists could combine electronic and physical attacks to disrupting emergency services at the same time as mounting a bomb attack.

Risk management analysts are focusing on the financial impact on businesses and economies [[8][4]]. They believe that an online attack would undermine public confidence in vital industries, especially utilities. A cyber attack on the electricity or nuclear power industry would cause communications operations to close down for a period, expose customers to loss of service, increase liability exposure and ultimately damage reputation for service delivery.

Western nations are not alone in their fear of a digital meltdown. The Malaysian government recently announced plans to establish a centre to fight cyber-terrorism. The hope is that the centre will provide an emergency response to hi-technology attacks around the globe. This facility is to be

located outside Kuala Lumpur and named the International Multilateral Partnership against Cyber-Terrorism, or Impact, and would be funded by a combination of government revenue and the private sector.

Malaysia sees the threat of cyber-terrorism as very serious. with potential to wreak havoc and cause disruption to people, governments and global systems .A cyber-attack can CAUSE a nationwide blackout, a collapse of trading systems and the crippling of a central bank's cheque clearing system.

The Governments worldwide on preparations for the Millennium bug spent almost £400m. Computer consultants issued dire warnings of the danger of an information technology breakdown that could paralyse nations on New Year's Day 2000. and some are not taking a potential cyber attack very seriously because nothing happened after preparations for a Millennium bug attack.

A simulation in 2002 by the US Naval War College concluded that an electronic Pearl Harbour-type- attack on America's infrastructure would certainly cause serious disruption. However, since such an attack would require five years of preparation and a \$200m budget. it is not likely to happen.

Reports of security studies reveal that computer security officers at a number of chemical plants are very concerned about the openness of their networks. The US has allocated a budget of \$93m budget for 2007 to the Department of Homeland Security to defend against cyber attack. The question to be asked is, how secure can any system be if thousands of people and thousands of data ports can provide inside access to that system?

The threat from software

IT security consultants Cyber Defence Agency (CDA) has warned the US military, government against using outsourced commercial software, which could be tampered with by terrorists. CDA said that gas, electricity, telecommunications, banking and water companies are among the services that could fall foul of cyber terrorists exploiting life-cycle weaknesses buried deep in the software code. Life-cycle attacks occur when one line of code is programmed to open vulnerabilities within the software, exposing the software and the company to external threats. The chances of strategic damage from a cyber-terrorist attack on the US increases the longer it takes to remedy the risks posed by outsourced software.

Internet security experts are holding many security conferences this summer^[9]_[5]. They are alerting organisations that terror attacks of 11 September 2001 and 7 July 2005, might be mere staging posts compared to what is planned.

Identity theft is another computer crime

Computer crime today consists of identity theft, as well as

*Cyber blackmail [DDoS, HIJACKING]

*Trojan-diallers [premium numbers]

*Theft of virtual property [such as online games]

***Adware [pop-up banners, Trojan downloaders]**

***Pornware [diallers, downloaders]**

***Illegal encrypting of your files without your permission, using a virus, which uses the RSA algorithm to encrypt files.**

***Financial fraud by way of ONLINE BANK TROJANS, PHISHING, PHARMING[10][6] and NIGERIAN LETTERS.[11][7]**

Examining the facts show that in December 2002 in the United States, records for more than 560,000 troops, dependents and retirees were stolen from computers at a health care provider in Arizona.[12][8]

In May 2006, in the United States the theft occurred of 26 million veterans' personal information from a Department of Veterans Affairs employee's home, Several U.S. military computers containing personnel records were found for sale at a bazaar outside a U.S. base in Afghanistan, according to an April report in The Los Angeles Times, which stated:" Thieves broke into a Colorado? Facility in September 2005, making off with personal information belonging to deployed soldiers."

Vigilance is the key

Be very careful with your personal information on-line

Try not to use the same online computer when you are writing letters, balancing your book-keeping accounts, or keeping passwords and asset details for online surfing

Encrypt your data...

If you do become a victim of identity theft, these are useful steps to take:-

A. Contact the fraud departments of any one of the three consumer reporting companies to place a fraud alert on your credit report. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts.

B. Close the accounts that you know or believe have been tampered with or opened fraudulently.

C. File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or at the very least, the number of the report, to submit to your creditors and others that may require proof of the crime.

How does cybercrime help fraudsters?

In the banking sector, although account opening procedures and front-end screening tools provide a solid level of protection, the most determined fraudsters still find ways to circumvent these efforts. While it often is not possible to avert a loss due to a new method or scheme systems can be developed to prevent offences that are often repeated and copied.

Fraud Screening is a service that helps detect name- fraud and identity-theft by identifying criminals moving from one financial institution or industry to another. Facilitating the sharing of data used to perpetrate a known fraud, fraud screening systems act as Trusted Custodians, maintaining and safeguarding certain information for the sole purpose of preventing fraud losses.

Keep Incident records

Each incident record represents identifying information used during a known or attempted fraud. Incident records fall into one of five general categories: Loan, Card, Check, Fund Transfer and Identity Fraud. Additional victim records are also maintained to safeguard the identity of those subjected to identity theft.

There are several factors that have contributed to the overall success of Known Fraud Prevention:

Operating Rules - To maintain the highest data integrity, participants agree and adhere to a common set of rules governing data submission and usage policy

Revenue Sharing - Rewards contributors when information they provide results in a warning

Historical File Search - To detect fraudulent individuals that have already compromised an institution's defences, the system retroactively compares any new fraud incidents to an existing customer base

Dispute Resolution - Gives consumers an opportunity to resolve any mistakes and establish that they are the victim, not a perpetrator

Victim Protections - Proactively protects individuals from further misuse of their identity by providing a way to denote their victim status

Full compliance.

In the past year in the banking sector there have been over 5,000 exact matches to these incident records, with each match representing avoidance of a potential loss

Banks undertake data mining

An examination of e-mails and data preservation is necessary as well as mining and data harvesting. and this is the costliest phase of electronic data discovery. Scouring servers, local hard drives and portable media to gather files and metadata is a very expensive undertaking and demands a threshold decision: of whether all or some files are to be mined relevant files, what materials are to be sifted for.

For example, when a corporate defendant asks employees to segregate responsive e-mail, or a paralegal goes from machine-to-machine or account-to-account selecting messages, the results are "field filtered Field filtering keeps costs down by reducing the volume for the solicitor's review, but it increases the risk of repeating the collection effort, loss or corruption of evidence and inconsistent selections. If keyword or concept searches alone are used to field filter data, the risk of under-inclusive production skyrockets.

Initially more expensive, comprehensive harvesting, unfiltered but defined by business unit, location, custodian, system or medium, saves money when new requests and issues arise. A comprehensive collection can be searched repeatedly at little incremental expense, and broad preservation serves as a hedge against spoliation sanctions. Companies embroiled in serial litigation or compliance production benefit most from comprehensive collection strategies.

A requesting party cannot frame effective keyword searches without knowing what the crux of the issue is... Strategically, a producing party requires an opponent to furnish a list of search terms for field filtering and seeks to impose a "one list, one search" restriction. The party seeking discovery must either accept inadequate production or force the producing party back to the well, possibly at the requesting party's cost.

Any harvest method must protect evidence integrity. A competent tracking of e-evidence is necessary- the e-system, custodian, folder, file and dates. There is more to e-mail than what you see on screen, so it is wise to pre-empt attacks on authenticity by preserving complete headers and encoded attachments.

Be prepared to demonstrate that no one tampered with the data between the time of harvest and its use in court. Custodial testimony concerning handling and storage may suffice, but better approaches employ cryptographic hashing of data—"digital fingerprinting"—to prove nothing has changed.

METADATA

There is more to an e-mail than its contents: there is metadata, too. Each e-mail is tracked and indexed by the e-mail client ("application metadata") and every file holding e-mail is tracked and indexed by the computer's file system ("system metadata").

E-MAIL METADATA

E-mail metadata is important evidence in its own right, helping to establish when a message received, read, forwarded, changed or deleted, is genuine and not a forgery. Metadata's evidentiary significance garnered scant attention until

System metadata is particularly fragile. Just copying a file from one location to another alters the file's metadata, potentially destroying critical evidence. Ideally, your data harvest should not corrupt metadata, but if it could, archive the metadata beforehand. Though unwieldy, a spreadsheet reflecting original metadata is preferable to spoliation. EDD and computer forensics experts can recommend approaches to resolve these and other data harvest issues.

PROCESSING AND POPULATION

However scrupulous your e-mail harvest, what you have reaped is not ready to be text searched. It is a mish-mash of incompatible formats on different media: database files from Microsoft Exchange or Lotus Domino Servers, .PST and .NSF files copied from local hard drives, HTML fragments of browser-based e-mail and .PDF or .tiff images. Locked, encrypted and compressed, it is not text, so keyword searches fail.

Before search tools or reviewers can do their jobs, harvested data must be processed to populate the review set, i.e., deciphered and reconstituted as words by opening password-protected items, decrypting and decompressing container files and running optical character recognition on image files. Searching now will work, but it will be slow going thanks to the large volume of duplicate items. Fortunately, there is a fix for that, too.

E-MAIL- SOME FACTS

***Nearly five billion dollars was spent by United States companies in 2005 in internally inspecting and analysing e-mails.**

***Over fifty percent of all evidence that is e-mail evidence**

***The number of outside e-mails that Microsoft Corp. receives daily is over 25 million.**

***Fifty-nine percent of companies in a survey that did not have e-mail retention policies.**

*** There are at least 100 legal matters in a typical Fortune 500 company, with at least 75 percent of them requiring e-discovery.**

***The amount in dollars that U.S. firms will spend on outside e-discovery services in 2006 in total is expected to be over two billion dollars.**

***Sixty two percent of surveyed companies doubt they can prove in a court of law that their e-records are accurate and reliable.**

*** Ten percent of US corporate lawyers reporting their businesses settled a case rather than incur the cost of e-discover**

*** There are over two hundred backup tapes at Microsoft being recycled every two weeks. It would cost \$1.7 million per year to save them.**

*** The former banker Frank Quattrone received a 18 month prison sentence for sending an e-mail telling Credit Suisse First Boston employees to “clean up” their files during a criminal inquiry of the bank.**

ELECTRONIC DISCOVERY

Several court opinions and rules have focused on the obligations of inside and outside LAWYERS in this phase of litigation. Failure to understand and fulfil these obligations can result in a critique of the lawyer’s performance in a court opinion, severe sanctions for the client. The obligation to locate and preserve evidence in electronic form is no different from the obligation to do so with respect to hard copies, an obligation with which companies and THEIR LAWYERS have lived for decades... Charges of spoliation - the intentional or negligent destruction of evidence - have overshadowed the merits of some cases and resulted in judgments or settlements that otherwise were unlikely to occur. A number of companies, such as Morgan Stanley, and UBS, have paid a price and received adverse publicity from their shortcomings with electronic discovery.

Lawyers’ failures in the Zubulake case –a lesson for the US as well as the UK

Lawyers are responsible for coordinating their client's discovery efforts.

Lawyers should adequately communicate with potential witnesses as to how to store data, and to produce their files, and they must ensure that certain relevant backup tapes are preserved.

It is the responsibility of counsel to advise their clients about those obligations.

Court Rules Impose Obligations

The Zubulake standard for litigation communications and collections[13][9] has become black letter law and has been cited and referenced in numerous cases since Zubulake was issued. The following is a sensible checklist:-:

***Enable your "discovery liaison" to readily describe information custodians, systems, storage, and your retention policies**

***Affirmatively and repeatedly communicate legal holds to all affected parties**

***Integrate your retention policies**

***Manage and monitor document collections**

***Interview to determine sources of information**

***Monitor compliance on an ongoing basis**

***Fully document the efficacy of your process**

*** Take responsibility for collecting and preserving all documentation.**

***Evaluate and constantly improve your processes**

***Review litigation documentation destruction policies and procedures**

*** Identify who is responsible and where information is stored and then close any knowledge and process gaps**

***Analyse for completeness, your system for collection of documents**

***Enhance your related record keeping for these purposes**

***Make sure you can retain collected documents (and your process records) as a part of the request and case record keeping**

***Educate senior business and IT executives on the changing risk profile and standards**

PSS Systems' Litigation Communications & Collections solution is the first and only software to specifically address the above 'Zubulake' checklist. It was designed with expert input and counsel from the United States top ten law firms and leading litigators. [14][10]

Locate Smoking Guns in Cryptic Messaging

Collecting documents in response to internal investigations or civil litigation discovery requests has always been a challenge. The problem is not so much gathering the documents (though volume can be problematic), but rather identifying the data repository nooks and crannies where important information may be stored.

Most difficult of all: The collecting party must develop logical and reproducible procedures for identifying relevant documents and separating them from the vast amount of other unrelated material. One particular challenge is sorting through e-mail messages and short messages sent from portable devices.

Blackberrys, text-enabled cell phones, text pagers and “smart phones” (Treos, etc.) have become convenient tools. Like the telegrams of old, these messages use the fewest possible words and letters to express the sender’s ideas, directives and responses, adding “emotions” to convey mood and emotion. Indeed, users on the go often write in a code that cannot be easily deciphered by anyone outside the immediate conversation thread. Messages written by thumb are usually cryptic; few e-mail messages clearly lay out players, issues and concerns. Instead, they may be quick responses to urgent e-mail messages; short directives in response to a phone call; or reactions to received information. Because users continue existing conversation topics, reactive messages tend to use pronouns and contractions whenever possible to save keystrokes. The result is a message that usually makes sense to recipients but contains enough ambiguous language that not anyone outside the conversation may understand its meaning, much less its significance. Current data collection techniques tend to overlook messages created by portable devices. Filtering e-mail by key word rarely finds matching terms in short messages that are full of creative abbreviations and misspellings.

Similarly, when documents are distributed to a litigation team for analysis, procedures to determine document relevance normally focus purely on the text of the document. E-mail messages that consist of odd phrases like, “OK 2 meets 2day?” and “CU at the usual place” may not appear relevant in this context. Notwithstanding their brevity, short messages can nonetheless convey a great deal of information. A CEO may agree to important contract revisions in an e-mail message that states, “OK by me” or “K OK.” A criminal act may be triggered by the message, “I’m ready.” Each of these messages, if they are properly understood, can provide solid proof of unrecorded conversations or the culmination of many related actions.

The challenge facing law firms’ document review teams is to find a way of deciphering short messages to assess their overall significance. Perhaps the best way to decode the meaning of short messages—or any document that is not self-explanatory—is to view the document in a larger context of related information. For e-mail messages in a discovery document collection, this may be as simple as reviewing e-mail messages that have been organized into individual conversations, rather than looking at the collection in strict chronological order, when many unrelated conversations may be occurring simultaneously.

Following dedicated e-mail threads from start to finish permits a reviewer to see how vocabulary evolves over the life of a conversation. In addition, seeing the full life cycle of an e-mail thread may make it easier to understand the perspectives of each participant in the message and may provide

additional areas to investigate.

At a more subjective level, understanding the conversation that was taking place between one set of individuals may better inform the document reviewer as to the context for other separately threaded conversations. Additional contextual information can also help unlock the meaning of cryptic messages and documents.

E-mail is influenced by far more than other e-mail messages. Meetings, telephone calls, documents written or received and current events are only some of the external triggers for reactive communications. Understanding an author's other actions immediately before and after writing a message may shed additional light on the true meaning of terse or ambiguous language. Activities can be tied together by reviewing telephone call logs and by using document metadata to identify what documents may have been open on someone's computer while they were writing a specific e-mail message.

CONTEXTUAL ANALYSIS

Contextual analysis works. In the context of documents, e-mail messages, and other information sent and received by any executive, the conclusion could be reached that the executive was aware of financial irregularities within the company, for example. Properly executed contextual search involves tying together large amounts of disparate data. This is not an easy task, and is one that would likely be close to impossible without extensive use of complex logic and powerful computers. Only a few litigation support experts currently offer comprehensive contextual search services for electronic documents.

Problems, which abound in the united kingdom legal industry

Every few years the legal industry must adapt its document review and production processes to accommodate new tools and techniques. From managing paper-based document collections in boxes, to creating document indexes with desktop databases, to today's complex applications that combine document review and case management tools, each transition requires more skilled personnel and greater technology investments.

Increasingly, clients are demanding better, faster, cheaper delivery of legal services. To enhance productivity. To stay competitive, firms must meet these demands.

Here are some electronic data discovery challenges that your firm will soon face:

In-house or outsource?

The transition from paper-based discovery to Electronic Document Discovery [EDD] requires changes in skill sets, tools and supporting technology not readily available within most law firms. Practice support teams must have greater access to knowledgeable technology resources.

EDD goes beyond "electronic messaging" or "server-based file storage." Discovery requests can include databases, financial accounting systems, customer-facing business-to-business applications, and manufacturing and process control. These systems can be embodied in distributed databases and include Web interfaces, sales management systems and knowledge management tools.

Legal teams must be able to interact with client information technology resources to identify where relevant information is stored and how to extract required data. The legal teams must also understand complex data structures, proprietary development environments, and unfamiliar storage mechanisms. Collecting and processing paper-based document sets means working with a single medium—paper.

By contrast, extracting, processing and validating electronic collections necessitates working with many different mediums—and coordinating the information flow and processing from many different systems requires strong project management skills.

Handling these loads will be challenging at best.

Bibliography

Bruce.E.May et al, ‘The differences of Regulatory models and Internet Regulation in the European Union and the United States’, InformationandCommunicationsTechnology Law, Vol.13. No.3, 2004.

Glenn E.Curtiss et al, ‘Nations hospitable to organised crime and terrorism’, Trends in Organised Crime/Vol 8, No. `1, Fall 2004.

Conrad Jacoby,’Law Technology News’, September 15, 2005

Identity Act 2006, United Kingdom.

**James.H.Pierce, ‘Diagramming crash-crime scenes in 3-D proves quick, accurate, powerful in court’
Policeone.com website as at 06.06.2006.**

**Lou Reda Productions, ‘WWII Terrorist Tactics Exposed in Military Channel's Target America’,
Military.com, May 30, 2006**

Digital Evidence

By Sally Ramage

This is the type of digital evidence report that is valid in a court of law and which can be used in court, the digital evidence expert having used such scrupulous procedures, that his report is utterly valid and carries great weight.....

Developments worldwide have made it simple to acquire all sorts of information through the use of computers. Criminal activity is a major one. In an effort to fight an exponentially increasing fraud wave, law enforcement agencies, financial institutions, investment firms and insurance firms are

incorporating computer forensics into their infrastructure. From network security breaches to corporate money laundering, the common bridge is the demonstration that the particular electronic media contained the incriminating evidence.

Supportive examination procedures and protocols are used in order to show that the electronic media contains the incriminating evidence. The computer investigation process expands from the crime scene through analysis and finally into the courtroom. This summary of procedures attempts to inform about digital evidence reports.

Examination Of Digital Evidence.

Technology is advancing at a rapid rate, nevertheless, each case is unique and the judgment of the examiner should be given deference in the implementation of any particular procedures. Circumstances of individual cases and relevant laws may also require actions other than those described here.

When dealing with digital evidence, the following general forensic and procedural principles apply.

Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.

Persons conducting an examination of digital evidence should be trained for that purpose.

Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review. The aim is to conduct an accurate and impartial examination of the digital evidence.

Digital evidence is processed by assessment and computer forensic examiners assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take. Digital evidence, by its very nature, is fragile and can be altered, damaged or destroyed by improper handling or examination. Therefore, examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence. The purpose of the examination process is to extract and analyze digital evidence. Here, extraction refers to the recovery of data from its media and analysis refers to the interpretation of the recovered data and presenting it in a logical and useful format. All actions and observations should be rigorously documented throughout the forensic processing of evidence. This will conclude with the preparation of a written report of the findings. A well-trained examiner understands that documentation is continuous throughout the entire examination process.

Computer forensics as a discipline demands specially trained personnel in order to produce sound digital evidence recovery techniques. These computer digital examiners must have policies and procedures a Mission statement in order to establish the parameters for operation and function. Their Mission Statement would incorporate the core functions of high-technology crime investigations, evidence collection, or forensic analysis. All such personnel must meet minimum qualifications and job descriptions. They must ensure that all software they use is properly licensed and must prove that they have maintained their skill and competence through ongoing training.

Firstly, when a digital evidence report is required, the nature of the crime, court dates, deadlines, potential victims, legal considerations, volatile nature of the evidence, and available resources must all be considered. Established guidelines for receiving, processing, documenting, and handling evidence will be to hand. Other forensic disciplines might be able to recover some other evidence, such as fingerprints on the hard drive, hair or fibres in the keyboard, and handwritten disk labels or printed material.

Even if the examiner is from a one-man expert concern, he must have developed processes for preserving and processing digital evidence and should never attempt to look for files on the original media because this will change the date and time stamps associated with those files and possibly affect other data on the media. Procedures to guide the technical process of the examination of evidence should be tested prior to their implementation to ensure that the results obtained are valid and independently reproducible. The steps in the development and validation of the procedures must be documented and include identifying the task or problem, proposing possible solutions, testing each solution on a known control sample and evaluating the results of the test and finalizing the procedure. Original evidence should never be used to develop procedures.

The digital evidence should be thoroughly assessed by reviewing case detail, nature of hardware and software, potential evidence sought, and the circumstances surrounding the acquisition of the evidence to be examined and there should be a discussion as to the possibility of pursuing other investigative avenues to obtain additional digital evidence, identifying remote storage locations and email addresses.

Consideration must be made of the relevance of peripheral components to the investigation. For example, in forgery or fraud cases consider noncomputer equipment such as laminators, credit card blanks, cheque paper, scanners, and printers.

A determination must be made of the potential evidence being sought (e.g., photographs, spreadsheets, documents, databases, financial records). A determination needs to be made of any additional information regarding the case (e.g., aliases, e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, user names. This information may be obtained through interviews with the system administrator, users, and employees. There must be an assessment of the skill levels of the computer users involved. Techniques employed by skilled users to conceal or destroy evidence may be sophisticated (e.g., encryption, booby traps, steganography). A priority is established of the order in which evidence is to be examined, determining the equipment needed. This assessment might uncover evidence pertaining to other criminal activity. In some cases, the examiner may only have the opportunity to do the following while onsite: identify the number and type of computers; determine if a network is present; interview the system administrator and users; identify and document the types and volume of media, including removable media; document the location from which the media was removed; identify offsite storage areas and/or remote computing locations; identify proprietary software; evaluate general conditions of the site; determine the operating system in question; determine the need for and contact available outside resources, if necessary and establish and retain a phone list of such resources.

Completion of an examination must take place in a controlled environment, such as a dedicated forensic work area or laboratory. Whenever onsite, the examiner must attempt to control the environment by considering the time needed onsite to accomplish evidence recovery and the impact on the business. Then he will prioritize the evidence (e.g., distribution CDs versus user-created CDs); determine how to document the evidence (e.g., photograph, sketch, notes), evaluate storage locations for electromagnetic interference, ascertain the condition of the evidence as a result of packaging, transport, or storage and assess the need to provide continuous electric power to battery-operated devices always remembering that digital evidence is fragile and can be altered, damaged, or destroyed by improper handling or examination.

Therefore he must document hardware and software configuration of the system; verifying operation of the computer system to include hardware and software and take care to ensure equipment is protected from static electricity and magnetic fields. He must also identify storage devices that need to be acquired. These devices can be internal, external, or both. He must document internal storage devices and hardware configuration and disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.

He must perform a controlled boot to capture CMOS/BIOS information and test functionality of boot sequence (this may mean changing the BIOS to ensure that the system boots from the floppy or CD-ROM drive), time and date and passwords. He must then perform a second controlled boot to test the computer's functionality and the forensic boot disk. He must boot the computer and ensure the computer will boot from the forensic boot disk. He must reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS. He must ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices. He must remove the subject storage device and perform the acquisition. When attaching the subject device to the examiner's system, he must configure the storage device so that it will be recognized. Removing the disks and acquiring them individually may not yield usable results. In laptop systems, the system drive may be difficult to access or may be unusable when detached from the original system. Older drives may not be readable in newer systems.

He must ensure that his storage device is forensically clean when acquiring the evidence. Write protection must be initiated to preserve and protect original evidence. He must investigate the geometry of any storage devices to ensure that all space is accounted for, including host-protected data areas. He must capture the electronic serial number of the drive and other user-accessible, host-specific data.

To extract and analyse digital evidence, he must prepare working directory/directories on separate media to which evidentiary files and data can be recovered or extracted. The physical extraction phase identifies and recovers data across the entire physical drive without regard to file system. The logical extraction phase identifies and recovers files and data based on the installed operating system, file system, and application.

During the physical extraction stage, the extraction of the data from the drive occurs at the physical

level regardless of file systems present on the drive. This will include keyword searching, file carving, and extraction of the partition table and unused space on the physical drive. Performing a keyword search across the physical drive will be useful as it allows the examiner to extract data that may not be accounted for by the operating system and file system.

The logical extraction of the data from the drive is based on the file system present on the drive and may include data from such areas as active files, deleted files, file slack, and unallocated file space. He must extract the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location. Analysis is the process of interpreting the extracted data to determine their significance to the case. Some examples of analysis that may be performed include timeframe, data hiding, application and file, and ownership and possession.

Timeframe analysis is useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual at the time the events occurred. By reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) files of interest can be linked to the timeframes relevant to the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed. By reviewing the system and application logs that may be present, ie. error logs, installation logs, connection logs, security logs, etc. may indicate when a user name/password combination was used to log into a system. Concealed data on a computer can be revealed by correlating the file headers to the corresponding file extensions to identify any mismatches. The presence of mismatches may indicate that the user intentionally hid data.

By gaining access to all password-protected, encrypted, and compressed files, an attempt to conceal the data from unauthorized users may be revealed. He must analyze the file metadata, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application that created it and placing the subject at the computer at a particular date and time that may help determine ownership and possession. Files of interest may be located in nondefault locations . Hidden data may indicate a deliberate attempt to avoid detection .If the passwords needed to gain access to encrypted and password-protected files are recovered; the passwords themselves may indicate possession or ownership. Contents of a file may indicate ownership or possession by containing information specific to a user.

Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination. All documentation must be complete, accurate, and comprehensive. Documentation must be contemporaneous with the examination, and retention of notes follows policy procedures.

The digital evidence reporter must take notes detailed enough to allow complete duplication of actions; including dates, times, and descriptions and results of actions taken; irregularities encountered and any actions taken regarding the irregularities during the examination; additional information, such as network topology, list of authorized users, user agreements, and passwords. He must document the operating system and relevant software version and current, installed patches.

He must have documented information obtained at the scene regarding remote storage, remote user access, and offsite backups.

His report will include date of report, descriptive list of items submitted for examination, including serial number, make, and model, identity and signature of the examiner, a brief description of steps taken during examination, such as string searches, and graphics, image searches and recovering erased files and conclusions. The details of findings must describe in great detail the results of the examinations and include specific files related to the request; other files, including deleted files, that support the findings; string searches, keyword searches, and text string searches; internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity; graphic image analysis; indicators of ownership such as program registration data; data analysis; description of relevant programs on the examined items; techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.

A list of supporting materials must be included with the report, such as printouts of particular items of evidence and digital copies of evidence. A glossary will be included with the report to assist the reader in understanding any technical terms used, with a generally accepted source for the definition of the terms, including appropriate references.

Digital evidence is the best evidence. It cannot be fabricated as one step reveals another. It can be reconstructed. It can only be dubious if there is conspiracy, perjury, or forensic incompetence.

[1][1] R.Jerrard, "Illegal Evidence: The Fruit of the Poisoned Tree", R R Jerrard 147 JPN 725 and [1983] CPU Digest 217

[2][2] 77 Eng. Rep. 194, 195 (K.B. 1604)

[3][3] William Blackstone, Commentaries on the Laws of England 223 (1769).

[4][4] "Privacy & prejudice: whose ID is it anyway?", New Scientist, pg 20, 17 September 2005.

[5][1] Indeed, this is nothing new as the following article relates.

'WWII Terrorist Tactics Exposed in Military Channel's Target America

Military.com | Lou Reda Productions | May 30, 2006

SILVER SPRING, Edythe memory of September 11, 2001, is still vivid in the minds of most Americans. Many believe it was the first time a terrorist plot succeeded on the U.S. mainland. However, there have been several successful terror attacks on America and numerous

plans that never made the headlines, either because they were never carried out or because the government kept them secret to avoid nationwide panic. TARGET AMERICA exposes several terror strategies hatched by the Germans and Japanese during the second World War that were successful and others that luckily were not.

During WWII, Germany and Japan used vastly different methods, but both were determined to strike the United States with state-of-the-art weaponry. Viewers learn of Japan's successful artillery shelling of Fort Stevens, Ore., as well as the "fugo" in 1944 – 9,000 rice-paper balloons the Japanese launched into the jet stream to cross the Pacific and deliver explosives and firebombs into the forests of the Pacific Northwest. Fortunately, the balloons dropped explosives during the wet season, so the intended forest fires never happened.

In 1942, Germany sent eight men into the United States to sabotage bridges and factories – specifically targeting aluminium production. Four men entered the country in New York, the other four in Florida. The leader of the saboteurs turned him in after arriving in America, foiling the destructive plans. TARGET AMERICA also explores Hitler's enduring dream of attacking the United States with schemes using long-range bombers, submarine-launched rockets and a first-of-a-kind intercontinental ballistic missile."

[6][2] It is now a criminal offence to employ persons not on the Identity Register. To be on the register, a person must give his full name, other names by which he is or has been known, date of birth, and place of birth, gender, address of his principal place of residence and address of every other place in the UK or elsewhere where he has a place of residence. This information can be had by way of a passport type photograph, his signature, his fingerprints and other "biometric" information about him.

[7][3] for example, [Com's TippingPoint™ Intrusion Prevention System:](#)

[8][4] The Financial Crime Conference in London in May 2006 [iir conferences]

[9][5] example is Information Age- Future of The Data Centre,London,June 2006.

[10][6] FALSE 'BANKS' PRETENDING TO BE BANKONE, HALIFAX, BANK OF AMERICA, PAYPAL, LLOYDS TSB.

[11][7] one example of a Nigerian fraud letter is as follows:-

DEAR SIR

REQUEST FOR URGENT CONFIDENTIAL BUSINESS RELATIONSHIP
RE: TRANSFER OF US\$31.5M US DOLLARS INTO YOUR ACCOUNT. AFETR DUE CONSIDERATION WITH MY COLLEGUES I DECIDED TO FORWARD TO YOU THIS BUSINESS PROPOSAL. WE WANT A RELIABLE PERSON WHO COULD ASSIST US TO TRANSFER THE SUM OF THIRTY-ONE MILLION, FIVE HUNDRED THOUSAND U.S. DOLLARS ONLY (US\$31.5M) INTO HIS ACCOUNT. THIS RESULTS FROM AN OVER-INVOICE BILL...

Typed in capitals, the letter goes on to offer me 30% of the money for providing the necessary assistance and ends

LET HONESTY AND TRUST BE OUR WATCHWORD THROUGHOUT THIS TRANSACTION AND YOUR PROMPT REPLY WILL BE HIGHLY APPRECIATED.

BEST REGARDS, DR. OBI PATRICK.

[12][8] New York Times

[13][9] Michael.C.S.Lange, of Kroll Ontrack, who is a lawyer specialising in electronic evidence cases, said this of the case *Laura Zubulake v USB Warburg LLC, USB Warburg and USB AG, 02 Civ 1243 [2003] US*, *The court defence counsel was partly to blame for the*

document destruction because it had failed to duly locate relevant electronic information, to preserve that information, and to timely produce that information...'

[\[14\]\[10\] http://www. PoliceOne com](http://www.PoliceOne.com)

6TH JUNE 2006, article about software used

'Diagramming crash/crime scenes in 3-D proves quick, accurate, powerful in court' ,By James H. Pierce ' ...If you are still drawing diagrams of crash and crime scenes by hand, chances are good that it is absorbing a lot of time and taking you away from other work duties. However, paper diagrams also have many limitations because they can be lost or misplaced, and are hard to update or share with other personnel. You may have been diagramming crime and crash scenes by hand for years, but various software programs on the market can automate these diagrams. The benefits are well worth considering:

- *Electronic diagrams are easy to read, clear, detailed and to-scale.*
- *Once completed, these diagrams can be saved like any other computer file and shared among police department personnel and with other law enforcement agencies.*
- *Electronic diagrams, once created, can be converted to a 3D format, which makes them easier to understand while offering a professional appearance. Consequently, they are highly effective in a courtroom.*
- *These diagrams usually can be created in half the time that it requires to draw a paper diagram.*

Diagramming software programs created specifically for law enforcement have been available since the early 1990s. However, back then police departments were highly resistant to adopting the software and stuck to creating diagrams by hand. The resistance has weakened considerably as thousands of officers handling an increasing number of crash and crime scene investigations are finding these software programs quick and easy to learn. They have discovered that electronic diagrams are superior in detail and accuracy to hand-drawn diagrams. ...The best advantage of an automated drawing program is if you can convert it from the 2-D diagram that you have created to 3-D. This not only brings the scene being diagrammed to life, but more importantly, the 3-D depiction verifies the accuracy of the scene's details.